## PATENT ABSTRACTS OF JAPAN

(11)Publication number:

2001-014441

(43) Date of publication of application: 19.01.2001

(51)Int.CI.

G06K 19/073 G06F 12/14 G06K 17/00 H04L 9/32

(21)Application number: 11-374788

(71)Applicant: MATSUSHITA ELECTRIC IND CO LTD

(22) Date of filing:

28.12.1999

(72)Inventor: HIROTA TERUTO

TATEBAYASHI MAKOTO

YUGAWA YASUHEI **MINAMI MASANAO** KOZUKA MASAYUKI

(30)Priority

Priority number: 11119441

Priority date : 27.04.1999

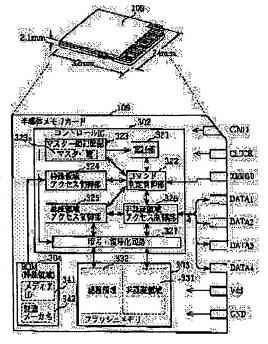
Priority country: JP

## (54) SEMICONDUCTOR MEMORY CARD AND READER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a semiconductor memory card usable as a storage medium for digital literary works and also usable as a storage medium for general computer data (non-literary works) for which the protection of copyright is not required.

SOLUTION: This card is composed of a control IC 302, a flash memory 303 and a ROM 304, the ROM 304 holds a medium ID 341 or the like peculiar to this card, the flash memory 303 has an authentication area 332 for permitting access to external equipment only when the authentication of that external equipment is made successful and a nonauthentication area 331 for permitting access regardless of the authenticated result and the control IC 302 has control parts 325 and 326 for controlling access from the external equipment to the authentication area 332 and the nonauthentication area 331 and an authentication part 321 or the like for executing mutual authentication with the external equipment.



(19) 日本国特群庁 (JP)

(12)公開特許公報 (A)

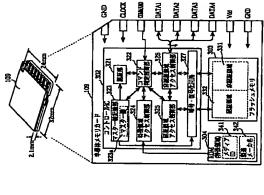
W ( ★ ) (11)特許出額公開番号

特開2001—14441 (P2001—14441A) (43)公開日 平成13年1月19日(2001.1.19)

19/073   19/073   19/073   19/073   19/073   12/14   320   12/14   320   4   17/00   17/00   17/00   19/32	(51) Int. C1.7		極別記号	<u>н</u>			,_	テーセュード(粉粃)	70年)
7/00 G 0 6 F 1 1 7/00 G 0 6 K 1 9/32 H 0 4 L 日本全計次 計2 日本		1,073		G 0 6 K	19/00			58017	
7/00 G 0 6 K 1 9/32 H 0 4 L # # # # # # # # # # # # # # # # # #		11/	320	G 0 6 F		0 2		58035	
9/32 H04L		00/		G 0 6 K	17/00			58058	
審査請求 未請求 請求項の数17 OL 特闘平11-314788 (71)出額人 平成11年12月28日(1999, 12.28) (72)発明者 号 特闘平11-119441 平成11年4月27日(1999, 4.27) (72)発明者 日本(JP) (72)発明者		37,35		H 0 4 L		7.5		53104	
毎至請求 未請求 請求項の数17 OL 特額平11-374788 (71)出額人 平成11年12月28日(1999, 12.28) (72)発明者 号 特額平11-119441 平成11年4月27日(1999, 4.27) (72)発明者 日本 (JP) (72)発明者					9	7 5	Д		
特別平11-374788 平成11年12月28日(1999.12.28) (72) 発明者 号 特部平11-119441 平成11年4月27日(1999.4.27) (72) 発明者 日本 (JP) (72) 発明者		審重計	米四米	TO			₹ 53	7月)	
平成11年12月28日(1999, 12.28) (72)発明者 号 特都平11-119441 平成11年4月27日(1999, 4.27) (72)発明者 日本 ( J P )	21) 出願番号	4	<b>374788</b>	(71)出題人	000005821	1: 1:	#		
9 特額平11-119441 平成11年4月27日(1999.4.27) 日本 (JP) (72)発明者	22) 出暦日	中	Q11年12月28日(1999.12.28)		大阪府門真和	17.14.14.14.14.14.14.14.14.14.14.14.14.14.		受佛900	
9 時間平11-119441 平成11年4月27日(1999.4.27) 日本 (JP) (72)発明者 (74)代理人				(72) 発明者	医田 照人				
平成11年4月27日(1999.4.27) 産業株式会社内 日本 (JP) (72)発明者 筋体 敵 大阪府門真市大字門真1 産業株式会社内 (74)代理人 100090446 弁理士 中島 司郎	31)優先権主張番号		4平11-119441		大阪府門真市	5大字	道	00644周	松下電器
12) 発明者 館林 麒   大阪府門真市大字門真    庭森株式会社内   (74) 代理人 100090446   142上 中島 司朗	32)優先日	日日	211年4月27日(1999.4.27)		面繁株式会社	£.			
大阪府門真市大字門真1 庭森珠式会社内 (74)代理人 100090446 弁理士 中島 司朗	33) 優先権主張国	#	K (JP)	(72) 発明者	紅木 就				
産業株式会社内 100090446 弁理士 中島 司郎					大阪府門真市	扩大字	<b>温度</b>	006年起	松下電器
100090446 弁理士 中島 司朗					庭欺株式会社	£.			
中島司郎				(74) 代理人	100090446				
							<b>55</b>	(外1名)	
								韓	の対しに称く

(54) 【発明の名称】半導体メモリカード及び配み出し装置

57) [聚秒]



【毎許部次の范囲】

【静水項1】 電子機器に遊脱可能な半導体メモリカードであって、

書き換え可能な不知路メモリと、

哲の不理等メモリ内の干め定められた20の配種資味である路配質機など非認配質域への前配電子機器によるアケセスを配卸する解却下る解認回路とを備え、

世紀監御回路中、

前記井路匠領域への前記電子機器によるアクセスを開卸する井路匠領域アクセス側御部と、 前部電子機器の正当性を後距するために前記電子機器の

部位を対みる際証券と、 が配配に対対して対して場合にだけ前配配値数等へ の対するこれ場が、ドックチェッを指示すと呼ばのはサッ

MERSHEW 1982年17月27日 MERSHENG の利用の電子機能によるアクセスを許可する配面機能で セス関節的と各有することを特徴とする非導体メモリカード・コード 【樹水填2】 前配製配部は、磐匠の結果を反映した観 データを生成し、 **前記版匠飯なアクセス部等的は、前記電子袋器から送られてくる暗中化された命令を前記器匠部が生成した段がれてくる暗中にされた命令に従って前記器匠廠様へ一夕で復与し、彼号された命令に従って前記器匠廠様へのアクセスを制御することを特徴とする請求項1記載のの平準体メモリカード。** 

「諸水項3」 前配配価的は、前配電子機器とチャレンジ・レスポンス型の相互認証を行い、前配電子機器の正当性を検証するために前配電子機器に送信したチャレンジデータと自己の正当性を証明するために生成したレスポンメデータとから前配線データを生成することを特徴とする諸水項2配銭の半導体メモリカード。

「耐水質4】 前配電子機器から送られてくる暗号化された命令は、前配路低額線へのアクセスの値別を修定する暗号化されていないタグ部と、アクセスする観線を特定する暗号化されたアドレス部とからなり、

が関係におけ、前に種グータを用いて、前配命令のアドレス部を復与し、値号されたアドレスによって参応される優略に対して、前配命令のダブ部によって参泛される優級のアクセスを実行労闘することを特徴とする議会項3 8階級の半端体メモリカード。

「酵水項5】 前配半導体メモリカードはさらに、他の 半導体メモリカードと区別して自己を特定することが可 能な固弁の機別データを予め配値する職別データ配億回 ※まかか。 前部級証的は、前部織別ゲーク配信回路に移納された職別ゲータを用いて相互認証を行い、前記織別ゲータに対存させて前配職ゲークを生成することを特徴とする語次項を出て前配職ゲークを生成することを特徴とする語次項を記載の半導体メモリガード。

【酵水項6】 約四半導体メキリカードはきらに、約四 8匹倒体及び前四非常匹回板それぞれの倒板サイズを受 更する倒様サイズ変更回路を備えることを特徴とする研 水項1配銭の半導体メモリカード。

特別2001-14441

8

2 7 - Average enter a character of the contract of the contrac

【辞女項1】 前配配証価核と前配非認証假核は、前配不審銘メモリなの一定サイズの道統した配価値核を2分して申られる4金関核に割り当たられ、

前の領域サイズ変更回路は、前四一定サイズの配路徴載を2分する投界アドレスを変更することによって前配路 配額は及び前配井昭広朗線それぞれの関戦サイズを変更することを特徴とする諸状項の配数はかイズを変更することを特徴とする諸状項の配数の半導体メモリカー

【様次項8】 哲院飯様ナイズ政更回路は、 10 哲院既庭殿後における諸理アドレスと参理アドレスとの が応令示す原原資施変数で一ブルと、 指配学既保護権における諸理アドレスと参照アドレスと の対応を示す非認正領略変換テーブルと、 前記電子機器からの命令に従って前記認証領域変換テー ブル及び前配認証領域変換テーブルを変更する変換テー ブル変更能とを有し、 市匹昭広倒株アクセス街部部は、前記昭四億株変換テーブルに基づいて前四電子機器によるアクセスを慰留し、前記井昭四億年フセス制造部は、前配井昭紅領域で竣20 テーブルに着づいて前記電子機器によるアクセスを贈留することを参覧とする諸状境7記銭の半導体メモリカー

「耐水頂り」 前記的記憶体及び和配非的記憶は、、大れぞれ、前記一定サイズの配換機を2分して毎られる物理アドンスの高・微域及び低い倒域に割り当てられ、前記大阪に関係を設か・一大小は、協理アドレスの昇原が 物理アドレスの昇原となるように協理アドレスと物理アドレスとが対応がけられ、

**村民邸任衛攻役やーブルは、後望アドレメの早間が参30 強アドレメの降品が表けられるように韓国アドレスとの独上 ドレスとの第一大・ストルのはのよったを発しする様々項 8 配包の半導体メモリガード、** 

FR型の干部なメモッカード。 【研水図10】 耐配半導体メモリカードはさらに、予めゲータが特徴された群み出し専用のメモリ回路を協えることを体数とする報水図1配館の半導体メモリカー 「昨来項」1】 前配路位領域及び前配弁総位領域は、 前配亀子機器にとって網み巻き可能な配貨領域と群み出 し専用の配信領域とからなり、

40 前配的物回路はさらに、前配電子機器が前配不爆発メモリにデータを替き込むためのアクセスをする度に乱撃を現住する乱骸発生器を有し、

前記数位函様アクセス制御部及び前記非数位函域オクセス制卸部は、前配当数を用いて前記データを暗号化し、得られた暗号化データを前配部み書き可能な配信機等に替き込むとともに、前配当数を前記時身化データに対応 づけられた前配酵み出し専用の配饱関域に替き込むことを物質とする請求項1配銭の半導体メモリカード。

「請求項12」 前記制御回路はさらに、 前配的監督域及び前記非認配倒域における論理アドレス

S

竹配亀子被器からの命令に従って世記奴数テープルを奴 と物理アドレスとの対応を示す変換テーブルと、 更する変換テーブル変更部とを有し、

前配移証領域アクセス制御部及び前記非路匝領域アクセ によるアクセスを制御することを特徴とする請求項1配 ス制御部は、前記交換テーングに基ムいて前記電子複器 我の中部存メモリカード。

とともに、前記邸証倒板及び前記非認証領域から読み出 [諸水項13] - 粒記制御回路はさらに、前配認加領域 及び前記非認証領域に書き込むべきデータを暗号化する されたデータを復号化する暗号復号部を有することを特 徴とする請求項1記載の半導体メモリカード。

[請求項14] 前配不御鴉メモリは、フラッシュメモ

しであり、

て、前記昭虹飯坂及び前記昭虹領域に存在する未消去の 匈域を特定し、その領域を示す情報を前配電子機器に送 る未消去リスト酢み出し部を有することを特徴とする詩 哲問題節回路などのに、哲的属子被認からの命令に絞ら **水項1記載の半導体メモリカード。** 

[請求項15] 前記数証前は、認証のために電子機器 を使用するユーザに対してそのユーザに固有の情報であ るユーザキーを要求するものであり、

**村記ューザキーを記憶しておくためのユーザキー記憶部** 有記載御回路はからに、

前配設証部による認証に成功した電子機器を特定するこ とができる戦別情報を配位しておくための機別情報配位

ら織別情報を取得し、その織別情報が前配織別情報記憶 前記認証部による認証が開始されると、その電子機器か いる掛合には、前記認証的によるユーザキーの要求を禁 止させるユーザキー要求禁止的とを有することを特徴と 的に既に格納されているか否か後重し、既に格納されて する際水頂1配数の半導体メポリカード。

【請求項16】 請求項1記載の半導体メモリカードに 格納されたデジタル著作物を試み出す賦み出し装置であ 前配半導体メモリカードは、非認配領域に、デジタル著 作物が格納されているとともに、認証徴域に、前配デジ タル若作物の銃み出しを許可する回数が予め格納され、 前記航み出し装置は、

\$

許可されている母合にのみ前配非認証領域から前配デジ 前配非認証領域に格納されたデジタル著作物を読み出す 際に、前記認証質域に格許された回数を試み出し、その 回数によって配み出しが許可されているか否か判断する

タル塔作物を試み出すとともに、既み出した前配回数を 対算して前記邸証領域に告き戻す再生手段とを備えるこ とを特徴とする既み出し装置。 S

[請求項17] 請求項1配載の半導体メモリカードに

格納されたデジタル著作物を既み出してアナログ信号に 再生する節み出し装置であって、

**号に再生可能なデジタル著作物が格納されているととも** 前記半導体メモリカードは、非認能倒域に、アナログ信 に、認証質域に、前配デジタル著作物の前配稿子機器に よるデジタル出力を許可する回数が予め格納され、 哲的院や田つ湫御 村町非路駐倒板に格被されたデジタル著作物を餌み出し てアナログ信号に再生する再生手段と、 前記数距倒核に格掛された回教を聞み出し、その回教に よってデジタル出力が許可されているか否か判断する判 2

**小暦号のまま外部に出力するとともに、読み出した前記** 回数を減算して前配配配領域に告き戻すデジタル出力手 許可されている場合にのみ前配デジタル著作物をデジタ 段とを備えることを特徴とする航み出し装置。

[発明の詳細な説明] [0001] [発明の属する技術分野] 本発明は、デジタル著作物等 を記憶するための半導体メモリカード及びその銃み出し 装置に関し、特に、デジタル著作物の著作檔保護に好適 な半導体メモリカード及び銃み出し装置に関する。

ន

[0002]

[従来の技術] 近年、マルチメディア・ネットワーク技 桥の発展により、者楽コンテンツ等のデジタル華作物が インターネット等の通信ネットワークを通じて配信され るようになり、自宅に居ながらにして世界中の音楽等に 接することが可能となってきた。例えば、パーソナルコ ンピュータ (以下、「PC」という。) で告張コンテン リカードに格赦しておくことで、必要に応じて音楽を再 生し楽しむことができる。また、このようにして音楽コ ンテンツを格納した半導体メモリカードをPCから取り ながら音楽を聴くこともできる。このような半導体メモ ツをダウンロードした後、PCに装着された半導体メモ 出して携帯型音楽再生装置に装着しておくことで、歩き 大きな記憶容量の半導体メモリを内蔵した小型軽量の便 リカードは、フラッシュメモリ箏の不揮発性で、かつ、 和なカードである。

て、半導体メモリカードにデジタル著作物を記憶する掛 テンツを暗号化しておく必要がある。また、PC等に標 **台、不正なコピーを防止するために、蝦等を用いてコン 静容付されて広く出回っているファイル街組ソフトウェ** アによっては他の配筒媒体等にコピーすることができな 【0003】ところで、このような電子音楽配信におい いようにしておく必要もある。

して、半導体メモリカードへのアクセスを専用のソフト ウェアでのみ可能とする方策が考えられる。例えば、P Cと半導体メモリカード聞での認証が成功した時にのみ 【0004】このような不正なコピーを防止する方法と 半導体メモリカードへのアクセスを許可することとし、

**専用のソフトウェアがないためにその認証に成功するこ** とができない場合には半導体メモリカードへのアクセス が禁止されるとする方法が考えられる。

[発明が解決しようとする瞑題] しかしながら、PCが ド導体メモリカードにアクセスするのに常に専用のソフ トウェアを所有していない不特定のユーザと半導体メモ リカードを介して自由にデータ交換し合うことが不可能 となってしまう。そのために、フラッシュATAやコン パクトフラッシュ毎の従来の半導体メモリカードが有し ていた利便性、即ち、専用のソフトウェアを必要とする ウェアでアクセスすることができるという利便性が得ら トウェアが必要とされるのでは、そのような専用のソフ ことなくPCに標準添付されているファイル管理ソフト れなくなってしまう。

[0006] つまり、専用のソフトウェアでのみアクセ ス可能な半導体メモリカードは、著作権保護の機能を有 する点でデジタル単作物の配御媒体としては適している が、汎用的な使用が困難であるために一般的なコンピュ **ータシステムにおける補助配修装置として使用すること** ができないという問題点がある。そこで、本発明は、こ のような問題点に鑑みてなされたものであり、デジタル し、略作権保護が必要とされない一般的なコンピュータ データ (幹塾作物) の配包媒体としても用いることが可 能な半導体メモリカード及びその既み出し装置を提供す **著作物の配馅媒体として用いることが可能であり、か** ることを目的とする。 [映虹を解決するための手段] 上記目的を遊成するため に、本発明に係る半導体メモリカードは、既子機器に着 脱可能な半導体メモリカードであって、香き換え可能な 2 しの間値倒換かめる節間倒換と非認即倒換への前記句 子機器によるアクセスを制御する制御回路とを備え、前 記制御回路は、前記非路証領域への前記電子機器による アクセスを制御する非認配倒板アクセス制御街と、前配 電子機器の正当性を検証するために前配電子機器の認証 だけ前記認証領域への前記電子機器によるアクセスを許 可する認証領域アクセス制御部とを有することを特徴と 不熔発メモリと、前配不御路メモリ内の予め定められた を試みる認証部と、前記認証部が認証に成功した場合に

予め格納され、前配館み出し装置は、前配非認証領域に に、前記認証倒核及び前記非認証倒域それぞれの倒域サ イズを変更する領域サイズ変更回路を備えてもよい。ま た、本発明に係る航み出し装置は、上記半導体メモリカ ドに格納されたデジタル芸作物を配み出す配み出し装 に、デジタル雑作物が格納されているとともに、認即倒 域に、前記デジタル著作物の既み出しを許可する回数が [0008] いいで、杉配半導体メモリカードはさち 間であって、哲院半導体メモリカードは、非認信領域

存置2001-14441

3

格納されたデジタル発作物を飲み出す際に、前配認証質 核に格納された回数を誇み出し、その回数によった読み 出しが許可されているか否か判断する判断手段と、許可 されている場合にのみ前配弁認証徴域から前配デジタル **着作物を筋み出すとともに、銃み出した前配回数を攻算** して前配配証領域に替き戻す再生手段とを備えることを

を介して音楽コンテンツ等のデジタル等作物をダウンロ ードするPCと、そのPCに着脱可能な半導体メモリカ 一ド(以下、単に「メモリカード」という。)の外観を [発明の実施の形態] 以下、本発明の実施の形態につい て、図面を用いて説明する。図1は、通信ネットワーク 2

イタ107は、PC102とメモリカード109とを電 ポード104及びスピーカ106等を協え、内蔵するモ て、このPC102が有するPCMC1A等のカードス ロット (メモリカードライタ挿入口105) にはメモリ 気的に接続するアダプタであり、そのメモリカード挿入 [0010] PC102は、ディスプレイ103、キー カードライタ101が挿入されている。メモリカードラ デムによって通信回換101に接続されている。そし

て、ユーザは、以下の手順を揺ることで、インターネッ を取得することができる。まず、ユーザは、所望の音楽 コンテンツを、通信回袋101を通じて、P C 1 0 2 内 部のハードディスクにダウンロードする。 音楽データは 暗号化されており、そのままではPC102では再生す ト上にもろコンテンシプロスイダが結択する抽楽ゲータ [0011] このようなシステムを用いることによっ **ロ108にメモリカード109が散発されている。** 

[0012] 再生するためには、ダウンロード元のコン アンツプロパイダヘクレジットカード等を用いてお金を 払っておく必要がある。支払いを済ますと、コンテンツ プロパイダよりパスワードと権利情報を入手することが できる。パスワードは、暗号化された音楽データを解除 **するのに必要な銀データである。福利情報は、PCでの** 再生可能な期間を示す再生期限等のユーザに許可された 再生可能回数や、メモリカードへの香き込み可能回数、 ることはできない。

プリケーション」という。)に対して、入年したパスワ は、PC102のスピーカ106から音楽を再生出力さ せる場合には、箸作権保護機能が付いた専用のアプリケ ーションプログラム (以下、このプログラムを単に「ア プリケーションは、権利情報を確認した後に、暗号化さ れた音楽データをパスワードを用いて復号しながらスピ **ードをキーボード104から入力する。すると、その7** 【0013】パスワードと権利債報を取得したユーザ - カ106を通じて音声として再生出力する。 再生条件を示す情報である。

【0014】また、権利情報としてメモリカードへの否

ಬ

き込みが許可されている組合には、そのアプリケーションは、暗号化された音楽データ、パスワード、権利債権をメモリカード109に審き込むことができる。図2は、このメモリカード109を配配媒体とする携帯型の発音再生装置(以下、「ブレーヤ」という。)201の外観を示す図である。

[0015]プレーヤ201の上面には、液晶数示節203と数作ボタン202が設けられ、手前回面には、メモリカード109を着設するためのメモリカード挿入口206及びPC102等と後続するためのUSB等の通留ボート213が設けられ、右側面には、アナログ出力増子205及びアナログ入力増子23等が設けられている。

【のの16】プレーヤ201は、メモリカード109Kも紡された音楽データ、パスワード、権利指権に基づいて、再生が許可されている状態にあるならば、その音楽データを試み出して復与した後にアナログ信号に変換し、アナログ出力結平204に接続されたヘンドフォン208を通じて音声として出力したり、再生中の音楽データをデジタルデータのままデジタル出力結子205に出力したりする。

[0017] また、このプレーヤ201は、マイク等を介してアナログ入力端子23から入力されるアナログの音声信号をデジタルデータに変換してメモリカード109に配験した。そのPC102によってグウンロードされた音楽データ、パスワード及びがイークの音楽データ、パスワード及びがイークの音楽データ、パスワードの0に記録することができる。つまり、このプレーヤ201は、メモリカード109に配録された音楽データの再生に関して、図1に示されたPC102及びメモリカードライタ107に置き換わる機能を右する。

トやプレーヤ201と接続するためのUSB毎を備える デバイス鐵1118や制御プログラム111b締を予め メモリカードライタ107、メモリカード109から鰭 コーダ118、伸張されたデジタル音楽データをアナロ 配售しているROM111、RAM112、ディスプレ み出された暗号化音楽データを復号するデスクランプラ -AAC (ISO13818-1) に確拠したAACデ [0018] 図3は、PC102のハードウェブ構成を イ103、通信回線101と接続するためのモデムポー 4、メモリカード109と内部パス214とを接続する 1117、賃号された音楽データを伸張するMPEG2 グ音声信号に弦技するD/Aコンパータ119、スピー カ106及びファイル管理ソフトウェアやアプリケーシ ョンを格納しているハードディスク 1 2 0 等から構成さ 赤すブロック図である。PC102は、CPU110、 画伯ポート113、キーポード104、内部パス11

[0019] このPC102は、ハードディスク120に結婚されたファイル管理ソフトウェアを実行することで、メモリカード109をハードディスクのように独立したファイルンステム(1S09293等)を有する補助配信装置として用いることができるだけでなく、ハードディスク120に結婚された上述の専用アプリケーションを実行することで、適信がート113のモデムなを介して通信回数101から音楽コンテンツ等をグウンコードしたり、メモリカード109と適相互配配を行なった後に音楽コンテンツ等をメモリカード109に結構して、メモリカード109に結構されている音楽コンデンツ等を誘力してスピーカ106に再生出力したりす

5、メモリカード109との相互認証を単行する認証回 レーヤ201のハードウェア構成を示すプロック図であ 1aや制御プログラム211b等を予め配値しているR 操作ボタン202、内部パス214、メモリカード10 路216、メモリカード109から飲み出された暗号化 音楽データを復号するデスクランプラ217、復号され た音楽データ伸張するMPEG2-AAC (1S013 818-7) に専扱したAACデコーダ218、伸張さ れたデジタル音楽データをアナログ音声信号に変換する **ル音楽データに変換をするA/Dコンパータ221、そ** のデジタル音楽データをMPEG2-AAC (1S01 3818-7)に存扱して圧縮符号化するAACエンコ 一ダ220、圧縮符号化された音楽データを暗号化する [0020] なお、ROM111に格割されたデバイス 後述するように、相互認証等に用いられる。図4は、プ る。プレーヤ201は、CPU210、デバイス壁21 OM211, RAM212, 液晶数示部203, PC1 D/Aコンパータ219、スピーカ224、アナログ入 ル出力端子205及びアナログ入力端子223から構成 力端子223から入力されたアナログ音楽信号をデジタ スクランブラ222、アナログ出力端子204、デジタ 02等と接続するためのUSB等の通信ポート213、 **戦111aは、このPC102に固有の秘密鍵であり、** 9と内部パス214とを接続するカード1/F部21 20

[0021] このプレーヤ201は、ROM211に待り 報された刨卸プログラム211bをRAM212にロードしてPU210に実行させることで、メモリカード109に格納されている音楽コンテンツ等を餌み出してスピーカ224に再生出力したり、アナログ入力強子233や通信ボート213を軽て入力された音楽コンテンツ等をメモリカード109に格納したりする。つまり、通常のブレーヤと同様に、個人的に音楽を容音したり再生したりして楽しむことができるだけでなく、PC102によりダウンロードされた電子音楽配信に係る(等件籍展別が返回とされる)音楽コンテンツの配像・再生もで

[0022] 図5は、メモリカード109の分類及びハードウェア権成を示す図である。メモリカード109は、何度も繰り返して書き込みが行える書き換え可能な不理強性メモリを内臓しており、その配節容量は54M Bであり、外部から3.3vの電級とクロック信号の供益を受けて影作する。また、メモリカード109は、厚さ2.1mm、終32mm、後24mmの直方体形状で、その図面に書き込み防止スイッチ(ライトプロテクトSW)を右し、9ピンの被形端子によって観気的に外部機器と後続される。

[0023] このメモリカード109は、3つの1Cチップ(コントロール1C302、フラッシュメモリ303、ROM304)を内容している。フラッシュメモリ303、ROM304)を内容している。フラッシュメモリ303に、一指消去型の存き換入可能が不解分エリであり、糖理的な配倍質をして、正当な機器であると認定することなくアクセスを許可する配倍質をである。 本庭 とすることなくアクセスを許可する配倍質をである 非路匝倒転331年を右する。こでは、路匝環境331年を行かる。こでは、路匝環境331年を指係環じ関わる重要なデータを格納するために、お作権保護に関わる重要なデータを格納するため、フランスイにおける補助配値装置として用いられる。なお、これち2つの配倍質域は、フラッシュメモリ303上の一定のアドレスを提昇として区分されている。

[0024] ROM304は、特殊優校と呼ばれる既み出し専用の配値優域を有し、このメモリカード109に固有の確別情報であるメディア「D341やこのメモリカード109にしている。なお、メディア「D341は、他の半導体メモリカードと区別して自己を特定することが可能な固有の歳別データであり、ここでは、機器間の相互認証に用いられ、認配領域332への不正なアクセスを防止するために使用される。

0025]コントロール1C302は、アクティブ寮 子(論理ゲート等)からなる制御回路であり、認証師3 21、コマンド判定制御部322、マスター観記協部3 23、特殊関域アクセス制御部324、認証関域アクセ ス制御部325、非認証徴数アクセス制御部326及び このメモリカード109にアクセスしようとする相手機 器とチャフンジ・フメポンス型の祖互認証を行う回路か あり、乱数発生器や暗号器等を有し、その暗号器と同一 の暗号器を相手機器が有しているか否かを検出すること によって、相手機器の正当性を認証する。なお、チャレ ンジ・レスポンス型の相互認証とは、相手機器の正当性 それに対して相手機器において自己の正当性を証明する 処理が施こされて生成されたレスポンスデータを相手機 器から受け取り、それらチャレンジデータとレスポンス データとを比較することで相手機器を認証することがで 暗号・復号化回路327年を有する。 認証部321は、 を検証するためにチャレンジデータを相手機器に送り、

**移図2001-1444**1

9

10 きるか否かを判断するという認証ステップを、双方の機 Badtatioのシェレルをを

器が抽互に行うことである。 [0026] コケンド対応監御部322は、コケンドア

100261コマンド中広島の部322氏、コケントに ソを介して入力されたコッツド (このメモリカード10 9~の命令) の貨費を判定し実行するプラード回路や副 御回路からなるコントローラであり、入力されたコマンドの貨費に応じて、各種構成原業321~327を制のする。コマンドには、ファッシュメモリ303のデータ を繋み・春き・指生するコマンドだけでなく、ファッツ 10 ュメモリ303を制御するためのコマンド(アドン公 間や未済去データに関するコマンド等)も含まれる。

[0027] 倒えば、データの配み音をに関しては、窓 配荷域332にプクセスするためのコマンド「SecuraRa ad address count」、「SecuraFrite address count」、「SecuraFrite address count」、「Frite address count」、「Frite address count」、「Frite address」は、飲み春色の対象となる一道のセクタ群の最初のセクの毎号であり、「count」は、飲み春きする合計セクタ製を示しまた、セクタは、メモリカード109に対してデータを飲み音する際の単位であり、ここでは、512パ

[0028]マスター軽配信約323は、相互認証の際に相手機器が用いたり、フランシュメモリ303内のデータを保障するために用いられるマスター離323mを予め配筒している。特殊関係アクセス制御部324は、特殊関係(ROM304)に格納されたメディア1D341時を競み出す回路である。

【0029】 認証領域アクセス制御部325及び非認証 モリ303の配配倒転332及び非認証領転331への ヤ201毎)との間でデータを送受信する。 なお、これ 分のパッファメモリを有し、蟄理的には(外部機器との きには、ブロック(32個のセクタ、16Kパイト)を のプロックを一括消去するとともに、パッファメモリ中 コマンド上でのアクセスは)セクタを単位として入出力 するが、フラッシュメモリ303の内容を書き換えると ゲータを書き換える場合には、フラッシュメモリ303 から歓当するプロックをパッファメモリに読み出し、そ の該当セクタを書き換えた後に、そのプロックをパッフ 倒域アクセス制御部326は、それぞれ、フラッシュメ データ番き込み及び簡み出しを実行する回路であり、4 **らアクセス制御街325、326は、内部に1ブロック** 単位として入出力する。具体的には、ある1個のセクタ **本のゲータピンを介して外部機器(PC102やプレ-**ァメモリからフラッシュメモリ303に書き戻す。 8

【0030】時母・復争化回路327は、認証契率アクセス前路第325及び非認応領域アクセス前部第326による開始の下で、マスター軽配信第323に格納されたマスター観3238年日には時代及び復争化を行う回路であり、フラッシュメキリ303にデータを申き込の路であり、フラッシュメキリ303にデータを申き込

င္တ

ε

折し、認証倒板332に格納されたパスワードを盈む等 ひ際にそのゲータを暗号化して告き込み、フラッシュメ モリ303からデータを試み出した際にそのデータを復 **身化する。これは、不正なユーザがいのメモリカード1** 0 9を分解してフラッシュメモリ303の内容を直接解 の不正行為を防止するためである。

を生成し各構成要素に供給する同期回路や、輝発性の配 [0031] なお、コントロール1 C302は、これち **士取な核成更聚321~327の他に、クロックピンか** 坊止するために、そのROM304をコントロールIC ら供給されるクロック値号に同期した内部クロック信号 位倒姫及び不知発性の配管倒坂等を有する。また、特殊 **倒坂 (ROM304) に格納されている情報の改ざんを** メモリ303に格納し、外部から暫き込みできないよう い。そのときに、暗号・復号化回路321で暗号化した 302の中に内蔵させたり、それらの情報をフラッシュ に特殊領域アクセス制御部324が制限をかけてもよ データを格赦することとしてもよい。

見たメモリカード109の記憶領域の種類を示す図であ 31の3つの倒板である。特殊領域304は航み出し専 [0032] 図6は、PC102やプレーヤ201から る。メモリカード109が有する配憶倒嫁は、大きく分 けて、特殊領域304と認証領域332と非認証領域3 用の領域で、この中のデータに対しては、専用コマンド 2叉はプレーヤ201とメモリカード109との間で怒 核へのアクセスについては暗号化されたコマンドを用い る。非認証領域331は、ATAやSCSI等の公開さ れたコマンドでアクセスできる、即ち、認証せずに読み しては、フラッシュATAやコンパクトフラッシュと同 じように、PC102上のファイル管理ソフトウェアや を用いて餌み出しを行う。 認証領域332は、PC10 毎きできる倒板である。 掠って、非路后倒換331に左 肛が成功した時にのみ睨み曲きができる倒板で、この個 データの既み告きが可能である。

る略作権保護の機能とを提供している。つまり、非認証 関版331には、著作権保護の対象となる音楽データが に格納された暗号化コンテンツ426を復号するための 置として機能と、電子音楽配信に係る音楽データに対す は無関係な一般的なデータであるユーザデータ427年 [0033] 3つの配位領域には、以下の情報を格納す ることとし、これによって、一般的なPCの補助配億装 暗号化された暗号化コンテンツ426や、著作権保護と が格納される。 昭証領域332には、非昭匹領域331 特殊倒板304には、88配倒板332にアクセスするた めに必要とされる情報であるメディア 1 口341が格赦 秘密職となる暗号化キー425が格赦される。そして、

れたメディア10341を眺み出し、それを用いて認証 【0034】 PC102やプレーヤ201は、まず、微 袖みたたメモリカード109の特殊倒換304に結構み

ラッシュメモリ303には、 怒怔倒城332や非認証倒

S

質域332に格約された暗号化キー425、福利情報を 再生が許可されていれば、非認証領域331にある暗号 取り出す。それら暗号化キー425や権利情報によって 化コンテンツ426を飲み出し、暗号化キー425で復 **导しながら、再生を行うことができる。** 

ータだけをPC102等でメモリカード109の非認証 質蚊331に歯き込み、そのようなメモリカード109 [0035] もし、あるユーザが不正に入手した音楽デ をプレーヤ201に装着して再生しようとしたとする。

しかし、そのメモリカード109の非路配徴核331に 音楽データが格納されているものの、 認証質域332に 対応する暗号化キー425や権利情報が存在しないため 利情報を伴わないで音楽コンテンツだけをメモリカード に、そのブレーヤ201は、その音楽データを再生する ことがかきない。これによって、正規の毎号化キーや権 109に複数しても、その音楽コンテンツは再生されな [0036] 図7は、PC102やプレーヤ201がメ いので、デジタル著作物の不正な複製が防止される。

セスにおけるルールを示し、 (b) は各関域のサイズの 変更におけるルールを示し、 (c) はメモリカード10 102やプレーヤ201は、このメディア1D341を モリカード109の各倒板にアクセスする際の制限やコ 9の個域を示す概念図である。特殊倒域304は、既み 出し専用の倒換であり、認能士ずに専用コマンドでアク ID341は、認証領域332にアクセスするための暗 **导化コマンドの生成や復号に用いられる。つまり、PC** 航み出し、これを用いて認証領域332にアクセスする レンドの形類を示す図でもり、(a) は各個機へのアク セスできる。この作殊倒恢304に格舶されたメディア コマンドを暗号化し、メモリカード109に送る。一

は、メディアID341を用いて、その暗号化コマンド 方、その暗号化コマンドを受けたメモリカード109 を復号し、解釈して実行する。

セスが可能となる倒域であり、その大きさは(YYYY ~第 (XXXX+YYYY) のセクタアドレスを有する ラッシュメモリ303を締成する全てのセクタそれぞれ [0038] 非認証領域331は、認証せずにATAや +1)個のセクタに相当する。 つまり、この影転倒域3 32は、閻理的には、第0~YYYYのセクタで構成さ セクタから構成される。なお、セクタアドレスとは、フ り、この非認証質核331は、簡理的にも物理的にも第 [0031] 杤局宣換332は、PC102やプレーヤ モリカード109との間で酩証が成功した時にのみアク れ、物理的には、フラッシュメモリ303の第XXXX で、その大きさはXXXX個のセクタに相当する。つま 0~ (XXXX-1) のセクタで構成される。 なお、フ 201毎のメモリカード109にアクセスする装置とメ に対してユニークに付された一連の番号のことである。 SCSI等の標準コマンドでアクセスすることが可能

岐331に生じた欠陥プロック(正常に前み書きできな い不良の記憶領域を有するブロック)を代替するための 交替プロックの集まりからなる代替プロック倒載501 が予め割り当てられることがある。

もよいし、特殊領域304にアクセスするコマンドを暗 て、欧ロ領域332と非欧田領域331それぞれの領域 スできるとしたが、不正なユーザからの解析を防ぐため 【0039】また、特殊質核304は認証なしでブクセ に、怒疽を行ってからでないとアクセスできないとして 号化してもよい。衣に、図1 (b) 及び (c) を用い サイズを変更する方法について説明する。 [0040] フラッシュメモリ303に設けられる認証 フラッシュメモリ303の全記位領域から代替プロック **飯核501毎を除いた固定値、即ち、(XXXX+YY** は、境界アドレスXXXXの値を変更することで、可変 質核332と非認証領核331との合計の配億容量は、 VY+1) 個のセクタ分であるが、それぞれの大きさ となっている。

認証を行う。これは、PCのユーザに広く開放されてい る標準プログラムや不正なアクセスを行うソフト等を用 いて簡単に大きさを変更することができないようにする [0041] 倒娘の大きさを双叉するためには、初めに ためである。酩怔を行った後は、鰕城変更の専用コマン ドで、非昭匝倒版331の大きさ(新たなセクタ数XX XX) をメモリカード109に迷る。

ンドを受け取ると、その値XXXXをメモリカード10 城332及び非認証領城331へのアクセス制御を実行 [0042] メモリカード109は、その飯協変更コヤ 9内の不超路な作業領域等に保存し、以降のアクセスに おいては、その値を新たな境界アドレスとして、認証額 する。つまり、フラッシュメモリ303上の物理的な第 0~XXXXのセクタを非認証領域331に割り当てる とともに、第XXXX~ (XXXX+YYYY) 各目の セクタを認証領域332に割り当てる。そして、そのよ **うな新たなメモリマッピングに基凸いて、アクセス制御** 部325及び326は、輸興アドレスと物理アドレスと を変換したり、領域を越えるアクセス違反の発生を監視 モリカード109を見た協合の (コマンド上での) デー タ空間におけるアドレスであり、物理アドレスとは、メ モリカード109のフラッシュメモリ303が有するデ したりする。なお、簡単アドレスとは、外的機器からメ **一夕空間におけるアドレスである。** 

**囲アドレスに新たな物理アドレスが対応するように対応** [0043] ここで、もし、娘界アドレスを小さくする ことにより、認証領域332のサイズを大きくした場合 には、変更前との輸理的な互換性を維持するために、認 証倒域332に格納されていた全てのデータを移動させ る等の手当てが必要となる。そのためには、例えば、境 を移動 (複写) させ、新たな境界アドレスから始まる論 **界アドレスの移動量だけアドレスの下位方向に会ゲータ** 

**帯域2001-14441** 

8

に格納されていたデータの指理アドレスを維持したま ま、そのデータ空間が拡大される。

図である。ここでは、PC102がメモリカード109 [0044] なお、領核效更のための専用コレンドにつ いても、不正なアクセスを防止する観点から、コマンド を暗号化して用いることとしてもよい。図8は、普洛尹 1)がメモリカード109に咎き込む動作を示すフロー -タ毎のコンテンツをPC102 (及びプレーヤ20 へ書き込む場合 (S601) を説明する。

ると、まず、メモリカード109からマスター離323 [0045] (1) PC102は、デバイス酸111a **フンジ・フメポンメ型の認信を行い、その認信に成功**す 等を用いて、メモリカード109の認証的321とチャ aを取り出す (S602)。

(2) 太に、専用コマンドを用いて、メモリカード10 9の特殊倒恢304に格納されているメディア1D34 1を取り出す (S603)。

と、いま取り出したマスター録323aとメディア1D ば、上配路証において、メモリカード109に送信した 341とから、音楽データを暗号化するためのパスワー **チャレンジデータ (乱数) を暗号化したもの等を用い** [0046] (3) 続いて、乱数を生成し、その乱数 ドを生成する(S604)。このときの乱数は、例え ន

(4) 得られたパスワードをマスター鍛323aとメデ イア1D341で暗写化し、暗号化キー425として認 ゲータ (時号化キー425) を送信するのに先立ち、駁 肛質核332に告き込む(5605)。このときには、

【0047】(5)最後に、音楽ゲータをパスワードで 虹倒恢332に書き込むためのコマンドを暗号化してメ モリカード109に送信しておく。

ホナフロー図である。 ににでは、メモリカード109内 の音楽データをプレーヤ201が再生する語合 (S10 暗号化しながら暗号化コンテンツ426として非認証徴 模331に格쵄していく (S606)。 図9は、音楽デ ータ棒のコンテンツをメモリカード109から競み出し **てプレーヤ201(及びPC102)で再生する動作を** 

チャレンジ・レスポンス型の認証を行い、その認証に成 1 a 毎を用いて、メモリカード109の認証部321と 功すると、まず、メモリカード109からマスター駐3 [0048] (1) ブレーヤ201は、デバイス邸21 1) を収明する。 \$

(2) 枚に、専用コマンドを用いて、メモリカード10 9の特殊領域304に格赦されているメディア1034 238を取り出す(S702)。

[0049] (3) 続いて、メモリカード109の認証 関域332から音楽データの時号化キー425を取り出 50 寸 (S704)。このときには、データ (暗号化キー4 (を取り出す (S703)。

25)の餌み出しに先立ち、昭配倒板332から餌み出 すためのコマンドを暗号化してメモリカード109に法

る (S105)。このときの復身化は、図8に示された (4) 毎られた暗号化キー425をマスター顧323g とメディアID341で復号化し、パスワードを抽出す ステップS605での暗号化の逆效数である。

で抽出したパスワードで復号しながら音楽を再生してい [0050] (5) 最後に、非認証領域331から暗号 32の暗号化キー425がないと復号することができな 化コンテンツ426を餌み出し、上記ステップS105 < (S106)。このように、メモリガード109の米 認証質疑331に格納された音楽データは、認証質域3 再生することができないので、その音楽データの著作権 い。 従って、たとえ不正に音楽データだけを別のメモリ カードにコピーしたとしても、その音楽ゲータを正常に は安全に保護される。

何しんなく。

の、暗号化の領略化に伴い、メモリカード109やプレ 用いられるデバイス概や暗号化アルゴリズム等を適切に **脳択して用いることで、一定の条件を描たした機器だけ** -ヤ201等の回路規模が小さくなるという利点が得ら [0051]また、認証に成功した機器だけがメモリカ に対してメモリカードの認証倒域へのアクセスを許可す その暗号化に用いられたパスワードをマスター鍵とメデ 471Dで暗号化し、暗身化キーとして80位数数332 に格型なれたが(S605)、 マスター解及びメガィア **一ドの認証領域へのアクセスが許可されるので、認証に** る毎の着作権保護が可能となる。なお、この例では、メ 1 Dのいずれかを用いて暗号化することとしてもよい。 これによって、暗号の強度が低下する恐れがあるもの モリカード109に暗号化コンテンツを配録する際に、

【0052】また、プレーヤ201やPC102片、窓 のマスター艇323aを埋め込んでおいてもよいし、マ し回数」を格粧した例と、「デジタル出力許可回数」を を取り出したが、予めプレーヤ201やPC102にそ スター戦3238を暗号化し、暗号化マスター戦として うなメモリカードの認証領域の活用例として、「試み出 特殊倒板304に格粧しておいてもよい。女に、このよ 低により、メモリカード109からマスター雌323g な狂した因かがす。

**いこでは、メモリカード109に格納された既み出し回** [0053] 図10は、プレーヤ201 (及びPC10 数812の範囲内でのみ、プレーヤ201が、メモリカ 2)がメモリカード109の昭臣倒旋に格納された戦み 一ド109の非認証倒版331に格納された音楽データ を音声信号に再生することが許可されている場合(S B 出し回数812を操作する動作を示すフロー図である。 01) について説明する。

20 [0054] (1) プレーヤ201は、デバイス概21

1 8 等を用いて、メモリカード109の認証前321と **ルナフンジ・フメヂンメ勁の認問を行い、 その認信に収** 功すると、まず、メモリカード109からマスター駐3 23 a を取り出す (S802)。

(2) 太に、専用コマンドを用いて、メモリカード10 9の年券**包**換304に格推されているメディア1D34 1を取り出す (S803)。

餌城332から音楽データの暗号化キー425を取り出 [0055] (3) 熱いて、メモリカード109の80F 25)の額み出しに先立ち、認証優換332から飲み出 す (5704)。このときには、データ (時身化キー4 すためのコマンドを暗号化してメモリカード109に送

1から暗号化コンテンツ426を読み出し、上記ステッ

する (5906)。その結果、その値が無制限なデジタ **ル出力を許可する旨の値である場合は、非認証領域33** プS905で抽出したパスワードで復号しながらデジタ

04)、パスワードを街田する(S905)。

ルな音楽データとしてデジタル出力増子205から出力 [0061] (3) 一方、デジタル出力許可回数913

**†** 5 (8909).

ないと判定し(S908)、アナログ出力による再生だ けを行なう (5908)。 つまり、非認証徴転331か ら暗号化コンテンツ426を飲み出し、パスワードで復

が0を示す場合は、もはやデジタル出力は許可されてい

(4) 次に、メモリカード109の認証領域332から 既み出し回数812を取り出し、その値を検査する(5 804)。その結果、その値が無制限な配み出しを許可 する旨の値である場合は、図9に示された手順 (S70 4~5706)と同様の手順に従って、音楽を再生する (88806~8808)

805)、再生処理を終了する (S809)。そうでな い場合は、その既み出し回数812を1つ成算し、その [0056] (5) 一方、観み出し回数812が0を示 す場合は、もはや再生が許可されていないと判定し(S 上記手順に従って、音楽を再生する(S806~S80 **結果を認証領域332に告き戻した後に(S805)** 

域332に、予め許可された再生回数を指定した読み出 し回数812を格散しておくことにより、プレーヤ20 1による音楽再生の回数をコントロールすることが可能 となる。これによって、例えば、レンタルCDやKIO 【0051】このように、メモリカード109の認証徴 SK始末等によるアナログ再生に適用することが可能と [0058] なお、節み出し回数812に代えて、「断 ことが可能な総時間を制限することもできる。また、回 数と時間とを組み合わせてもよい。さらに、飲み出し回 み出し時間」とすることで、音楽コンテンツを再生する 数812は、再生を開始してから10秒毎の一定時間を 組えて再生され続けた場合にだけ、その回数を減算して もよい。また、旣み出し回数812は、不正な改ざんを むぐために暗身化して格徴することとしてもよい。

[0059] 図11は、ブレーヤ201 (及びPC10 2) がメモリカード109の昭位倒板に格納されたデジ タル出力許可回数913を操作する動作を示すフロー図 ジタル出力軒回回数913の衛田内でのみ、プレーヤ2 された音楽データを飲み出してデジタル出力することが である。いいでは、メモリカード109に格勢のれた小 01が、メモリカード109の非認配倒換331に格納 【0060】 (1) プレーヤ201は、図9に示された 件可されている場合 (S901) について説明する。

ド109の物理的なデータ構造(セクタ及びECCプロ で、著作権者が指定した回数だけデジタル出力許可回数 を増やす機能を追加してもよい。 吹に、このメモリカー [0064] さらに、専作権者に代金を払い込むこと

4. おいしな をしない しんりんかんい。

ックの構造) について説明する。このメモリカード10 9では、フラッシュメモリ303に格赦されたゲータの パックアップと復元に伴う不正行為やデータの改ざんに **半う不正行為等を防止するのに好適なデータ構造が採用** されている。つまり、上述のような「簡み出し回数」や それら行為を実行する既にカウントダウンしていく方式 「デジタル出力許可回数」を認証倒収332に格制し、 では、次のような攻撃を受ける可能性がある。

[0065] つまり、フラッシュメモリ303全体の配 改さんすることで、不正に音楽再生を繰り返すことが考

図である。 ここでは、コントロール I C 3 0 2 の認証部 332及び非認証領域331に共通のデータ構造と、そ 321時が有する乱数発生器1003が発生するカウン のデータ構造に対応した既み審き処理のフローとを示す

0.5が割り当てられる。各セクタは、カウンター値で指 **딝作中を格能するための8パイトのECCゲータ100** 値を格証するための8パイトの時效徴核1001とから トのセクタ1004ごとに、16パイトの枯蛩倒凝10 対応するセクタに格納されている暗号化データの殴り酊 6と、その暗号化データの生成に用いられたカウンター 号化されたデータが格納される。 拡張領域1005は、

ンド母を用いて) アクセス可能な倒域はセクタ1004 だけであり、拡張倒収1005は、物理的に(メモリカ で、コマンド等を用いてセクタデータだけが改ざんされ ても、時変質域1007の内容は変更されることがない 【0068】なお、閻理的に(ユーザに関放されたコマ **一ドを試み告きする装置による制御として)のみアクセ** ス可能な領域である。このようなデータ構造とすること

シシュメモリ303の邸配領域332や非認証領域33 は、まず、PC102がメモリカード109にデータを [0069] 具体的には、PC102やプレーヤ201 は、セクタ1004ごとに、以下の手順に従って、フラ 1にデータを格納したり、既み出したりする。ここで 唐き込む場合(S1001)の年順を説明する。 を防止することができる。 **\$** 

**ータのまま出力することが可能な総時間を制限すること** 

始してから10秒等の一定時間を超えて出力され続けた ル出力許可回数 9 1 3 は、不正な改ざんを訪ぐために暗

さらに、デジタル出力許可回数 9 1 3 は、その出力を開 掛合にだけ、その回数を放算してもよい。 また、デジタ

もできる。また、回数と時間とを組み合わせてもよい。

デジタル出力軒 町回数 9 1 3 に代えて、「デジタル出力 許可時間」とすることで、音楽コンテンツをデジタルデ

[0063] なお、「餓み出し回数」の場合と同様に、

ンター値の発行を要求する。すると、メモリカード10 003で乱数を発生し (S1005)、その乱数をタウ (1) PC102は、メモリカード109に対してカウ 9内のコントロール10302は、内部の乳敷粘生器1

ន

発開2001-14441

リカード109と認証を行なった後にマスター鍵323 出し (5903)、暗号化キー425を取り出す (59 デジタル出力許可回数913を取り出し、その値を検査 単生の協合(S 101~S 105)と同様にして、メモ aを取り出し (S902)、メディア1D341を取り (2) 次に、メモリカード109の認証倒転332から

値データを外部の補助配管装置等にパックアップしてお いた後に音楽再生を繰り返し、それら回数が0となった 時点でパックアップデータを復元することにより、再び 音楽再生を繰り返したり、「甑み出し回数」そのものを えられる。従って、そのような行為を防止する手当てが

[0066] 図12は、メモリカード109の認能倒換 ター値が時変の鍵として利用される。

> (4) 航み出したデジタル出力許可回数913が0では し、その結果を認証領域332に番き戻した後に(59 07) 、非認証質模331から暗号化コンテンツ426

**号しながら音楽を再生する(S908)。** 

ない一定の制限回数を示す場合は、その回数を1つ減算

を額み出し、上記ステップS905で抽出したパスワー ドで復号しながら デジタルな音楽ゲータとして デジタル [0062] このように、メモリカード109の認証倒 域332に、予め許可されたデジタル出力の回数を指定 したデジタル出力許可回数 9 1 3を格納しておくことに の回数をコントロールすることが可能となる。これによ って、倒えば、レンタルCDやKIOSK越来等による デジタル再生への適用、即ち、メモリカードに配億した 音楽データのデジタルダビングを著作権者の了解の元に 指定した回数分だけコピーを許可するような選用が実現

五力組子205から出力する(S909)。

**【0067】フラッシュメモリ303には、512パ**ソ

より、プレーヤ201による告徴ゲータのデジタル出力

ので、それらの螯合性を利用することで、不正な改ざん

からパスワードを生成する (S1003)。

(3) 審き込むべき1セクタ分のデータをパスワードで暗号化しながら、メモリカード109に送る(51004)。このとき、暫き込むべきセクタを指定する情報や、暗号化に用いたカウンター値も一緒に送る(4)メモリカード109は、受け取った暗号化データ(4)メモリカード109は、受け取った暗号化データ

(4) メモングード10514、大つ吹つた場でにプラインで、指定されたセクタ1004に着き込む(5100

2

[0071] (5) その略号化データからECCを計算し、上配セクタに対応する並過倒転1005代、ECCデータ1006として審き込む (S1007)。(6) 続いて、上配路号化データととに受け取ったカウンター値を時収倒破1007に奪き込む (S1008)。次に、PC102がメモリカード109からデータを試み出す過合 (S1011)の手順を設明する。[0072] (1) PC102は、メモリカード109

に対して、セクタを指定するともにデータの群み出しを要求する。すると、メモリカード109は、まず、指定

されたセクタ1004の暗号化データだけを聞み出して PC102に出力し (S1016)、PC102は、そ の路号化ゲータを受け取る(S1012)。 (2) 次に、メモリガード109は、指定されたセクタ 1004に対応する垃圾飯様1005の砂煤飯様100 7に結前されたカウンター値を眺み出してPC102に 出力し(S1017)、PC102は、そのカウンター値を受け取る(S1013)。

ユスペンカー (3) 財み出したカウンター値と、既に取得しているマスター観2323a及びメディア「D34」とからパスワードを生成する(S1014)。

(4) そのパスワードを用いて、暗号化データを復与する(S1015)。ここで、もし、不正な改ざ人等により、セクタ1004のデータが変更されている場合には、時変領域1007から誘み出されたカウンター値との不整合が生じ、元のデータに億元されない。

[0074]にのように、フラッシュメモリ303内に、ユーザからは見えない (アクセスできない) 庭し飯様としての時変優短1007を設け、そこに結結されたカウンター値に放存したパスワードでデータを暗身化し結断することで、不正なユーザによるデータの改ざんを訪止することが、不正なコーザによるデータの改ざんをが止することができる。なお、ここでは、時変優略1007は、ECCを格納するための垃圾優略1005としたが、メモリカードの外部から審き換えができない領線であれば、フラッシュメモリ303内の他の優級に設け

【のの75】また、カウンター値は、乳酸でおったが、 型々と変化する時刻等のタイトー値としたり、ファンツ コメモリ3の3への軸を込み回数を示す値としてもよ

1. 次に、フラッシュメモリ303の路理アドレスと物型アドレスとの対応づけについて、毎主しい例を説明する。図13社、糖理アドレスと物理アドレスとの対応を変更する様子を示す図であり、(a)は変更前の対応関係、(b)は変更値の対応関係、(c)は(a)に対応する複数テーブル1101、(d)は(b)に対応する複数テーブル1101を示す。

[0076]ににて、変数テーブル1101は、全ての路程アドレス(ここでは、路程プロックの毎争)と各階程アドレスに対応する砂程アドレス(ここでは、フラッシュメモリ303を構成する砂程プロックの毎号)とを組にして配位するデーブルであり、コントロール1C302内の不解発な配位倒域等に保存され、認配倒接下かせ入前段部325年代の工程の下に又かた場面部325元はして整理と下してを照される。

[0077] メモリカード109にアクセスする機器は、メモリカード109中の物理的に存在するすべてのデータ空間 (フラッシュメモリ303を構成する全ての物理プロック) にデータを告き込めるのではなく、時間アドンバに3つて特定できる時間的なデータ空間 (論型カーック) にのみデータを告き込めるのではなく、時間メトングにのみデータを告さむことができる。この理由の一つは、フラッシュメモリ303の一部が破損し間み供きが行えなくなった場合に、その関係を置き換えるため。そして、そのような名フェーッを代替領域中の公司を受験人た出るので、その対応づけの変更を変換えたものであっても、その対応づけの変更を変換スープルに反映しておくことで、複数の道像する物理フェックかちなるファイルの機関的な連続性は推移されるので、外部機器に対しては発動性になかった。

[0078]ところが、複数のプロックからなるファイル母をメモリカード109に格納したり、削除したりすることを繰り返していると、倫理プロックのフラグメンテーションが増大する。つまり、図13(a)に示されるように、同一のファイルfileを構成する情報プロックであるにもあわらず、それらの論理アドレスが不道符となってしまう。

[0079] これでは、例えば、音楽ゲータをメモリカード109に結婚しようとしたときに、メモリカード109の路理的な道線優様にむけないので、各プロック毎にむき込みコマンド「Frite address count」を発行する必要があり、毎き込み速度が低下してしまう。同様に、部み出し動作においても、1個を構成する音楽データであるにも約わらず、イフロックをに誘み出しコマンド Read address count」を発行する必要があり、音楽データのリアルタイム再生の職能となってしまう。

【0080】この西題を解決する方法として、このメキリカード109のコントロール【C302は、外部機器からのコンドに基づいて、変換テーブル1101を申からのコマンドに基づいて、変換テーブル1101を申

20

21

き換える機能を有する。具体的には、コントロール1C302のコマンド判定制御的322は、変換テーブル1101を暫き換えるための専用コマンドがコマンドピンから入力されると、そのコマンドを解釈し、続いて送られてくるパラメータを用いて変換テーブル1101を曹れてくるパラメータを用いて変換テーブル1101を曹

[0081] その具体的な動作は、図13に示される適りである。いま、上記専用コマンドが送られてくも前においては、フラッシュメモリ303において、図13(コンパーに、フラッシュメモリ303において、図13(コンパーが113を構成するデータが存在し、物理アドレス1にファイル113を構成するデータが存在し、物理アドレス1でファインが113を構成するデータが存在し、物理アドレス1で表して、変換デーブル1101には、図13(c)に、物理アドレスと特理下ドレスと前型アドレスとは一数する内容が保持されているとする。つまり、物理アドレス上に対応は、第四アドレス上に対いても、ファイルfilsのデータが別のファイルfils1のデータに挟まれて結構されているとする。

[0082] このような状態を解消しようとうする外部 機器は、フラッシュメモリ303に対して、特定のファ イルfile1の連続性を確保する音を示す上記専用コマン ド及びパラメータを送る。すると、メモリカード109 のコマンド判定側線第32は、その専用コマンド及び パラメータに従って、変貌ケーブル1101を図13 (4)に示される内容に審き微える。つまり、フラッツ 図13(b)に示されるように変更される。 【0083】図13(b)に示された関係図から分かる ように、物理プロックの配置は変化していないにも拘わ らず、ファイルfile1を構成する2つの簡型プロックが 道様するように再配置されている。これによって、その 外部機器は、次回のアクセス以降においては、それまで よりも高速にファイルfile1にアクセスすることが可能 [0084]以上のような変換テーブル1101の変更は、簡細プロックのフラグメンテーションを解消するためだけでなく、フラッシュメキリ303の窓配飯総33と光窓配飯総33と光窓配飯総33と光窓配飯総33とれぞれたかりイズを選早する場合の物理であれる。このときには、サイズを小さくする質の物理プロックがサイズを大きくする質像の物理プロックとして割り当てられるように変換デーブル1101を書き換えるだけで落むので、高速な関集変更が可能と

[0085] 次に、このメモリカード109が有する未消去プロックに関する機能、具体的には、未消去リストコマンド及び指去コマンドを受信した場合の動作について設明する。ここで、未消去プロックとは、フラッシュメモリ303内の物理プロックであって、過去に審き込みが行なわれ、かつ、物理的に未消去状態となっているプロックをいう。つまり、未消去プロックは、次に使用プロックをいう。つまり、未消去プロックは、次に使用

**参照2001-14441** 

22

される (昏き込まれる) 前に一括消去が必要とされる物理プロックである。

[0086] また、未消去リストコマンドとは、コマンド対定制御的322が解釈及び契行可能なコマンドのひとつであり、その時点におけるフラッシュメモリ303に存在する全ての未消去ブロックの番号の一覧を取得さためのコマンドである。メモリカード109に使用されているフラッシュメモリ303は、音き込みを行う制にプロック単位での一括消去が必要とされるが、その領主も込む時にかがより馬選に奪き込むことができる。そこで、このメモリカード109は、その便宜を図るために、米消去リストコマンドと消去コマンドを外額総器に、未消去リストコマンドと消去コマンドを外額総器に

[0087] いま、フラッシュメモリ303は、図14 (a) に示されるような辞理プロック及び物理プロックの使用状態とする。ここでは、路理プロックの~2が使用中であり、物理プロックの~2、4及び5が未指士プロックとなっている。この状態においては、コマンド利2の 定触時割3と2クに保持されている来消去リスト1203は、水消生リスト1203は、フラッシュメモリ303を構成する生での物型プロックに対応することによる制御の下で、対応する物理プロックの消去状態に成じた値(消去減みの過台は"0"、来消去の過台は

[0088] 図14 (c) は、このような状態において PC102やプレーヤ201が未満歩リストコマンドと 30 落去コマンドを用いて辛前にプロックを消去する場合の 動作を示すフロー図である。なお、フラッシュメモリ3 03には、図14 (d) に示されるように、韓国プロッ クの使用状態を示すFAT (File Allocation Table) 等のテーブルが結婚されているものとする。

"1") が保持される。

ュメモリ303の輪組及び物理アドレスの対応関係は、

(0089) PC102やプレーヤ201等の分的機器は、例えば、メモリカード109へのアクセスが発生していないアイドル時間において、このメモリカード109に対して未指生リストコマンドを発行する(51201)。そのコマンドを受け吸ったメモリカード109のコマンド判定制の部322は、内部に有する未消去リスト1203を参照することで、状態値1が登録されている物理プロックの番号0~2、4及び5を特定し、その外部機器に流す。

(0090) (続いて、外部機器は、フラッシュメモリ303に格納された図14 (d) に示される韓国プロックの使用状態を示すテーブルを参照することで、韓理的に使用されていないプロックを特定する (ステップ5120) として、上記2つのステップ51201及び5120での場に、南亜町能なプロッ50 次、即ち、韓理的に不使用で、かつ、物理的に未得去な

グロック(ここでは、物理プロック4と5)を特定した後に(ステップS1203)、メモリカード109に対して、それらプロック4と5の番号を指定した消去コマンドを発行する(ステップS1204)。そのコマンドを受信したメモリカード109のコマンド判定制御部322は、アクセス慰問部325、326に指示を出す等により、指定された物理プロック4と5を一括消去すにより、指定された物理プロック4と5を一括消去す

(0091) これによって、もし、その物理プロック4と5への音き込みが発生した岩台には、その物理プロックに対する消去処理は不安となるので、高弦な音き込みが可能となる。次に、このメモリカード109が有する個人データの保護に関する機能、具体的には、メモリカード109が保護機能について提明する。ここで、個人データの保護機能について提明する。ここで、個人データとは、そのユーザを一意に確別する。ここで、個人データとは、そのユーザを一意に確別する。ここで、個人デルタとは、スモリカード109の窓匠関域332へのアセスが軒可された正規のユーザとしてメモリカード109に確別させるためのデータでもある。

「0092」このような場合において、認証領域332へのアクセスの度にユーザに対して約り返し個人データを入力することを要求したり、その個人データを認配領域332に存納することとしたのでは、不正者によって登場されたり、認匠領域332にアクセスする権限を有する他のユーザによってもられたりする不動合かる。「0093」これを防止するために、音楽データと同様に、個人データについても、個人が設定したパスワードで結合化してから格材するという方法が考えられる。しかしながら、パスワードを設定した地が考えられる。しかしながら、パスワードを設定した地が考えられる。しかしながら、パスワードを設定した地がはなな。そこで、このチェリカード109以、不必要に個人データを制り返し入力することを回避する機能を有する。

[0094] 図15は、認証のためのプレーヤ201とメモリカード109間の適倍シーケンス及び主要な構成要素を示す図である。なお、本図に示される処理は、主にプレーヤ201の認証回路216及びメモリカード109の認証的321によって実現される。本図に示されるように、プレーヤ201の認証回路216は、結号化及び復号化等の機能の他に、メモリカード109に保持されたマスケー醛323aと同一の秘密器であるマスケー配1301と、製造者号(s/n)等のプレーヤ201に固有の1口である機器固有1D1302とを予約配

[0095]また、メモリカード109の昭広部321 は、時号化、位号化及び比較等の機能に他に、2つの不 解発な配慮領域である機器固有1D韓配値領域1310 とユーザキー配値領域1311とを有する。機器固有1 D韓記値領域1310は、このメモリカード109の認

8

位倒な332~のアクセスが許可された全ての機器の機器の指数値付10を配修しておくための配修関係であり、ユーザキー配修関係1311は、個人データとして機器から込られてきたユーザキーを配修したおくための配修販権をよっま。

【0096】具体的な認証手順は、以下の適りである。 なお、送受信においては、全てのデータは暗号化されて 送信され、受信回で似号される。そして、手順が進む度 に、次の手順での暗号化及び似号化に用いられる輸が生 に、次の手順での暗号化及び似号化に用いられる輸が生 (1)メモリカード109とプレーヤ201とを接続すると、まず、プレーヤ201は、マスター録1301を 用いて機器固有1D1302を暗身化し、メモリカード109に送る。

成される。

[0097] (2) メモリカード109は、受け歌った暗号化された機器固有1D1302をマスター顧323aで値号し、得られた機器固有1D1302が既に機器固有1D1302が既に機器固有1Dは整色価額数1310に格納されているか検査す

(3) その結果、既に機器固有1D1302が結婚されている場合は、既配が成功した旨をプレーヤ201に適 知し、一方、機器固有1D1302が結婚されていない。場合は、プレーヤ201に対しューザキーを要求する。 [0098] (4) プレーヤ201は、ユーザキーの入力をユーザに促した後に、ユーザから個人データとしてのユーザキーを取得し、そのユーザキーをメモリガード109に送る。

(5) メモリカード109は、送られてきたユーザキーと予めユーザキー配管領域1311に結舶されているものとを比較し、一致している場合、又は、ユーザキー配信領域1311が空であった場合は、認証が成功した首をプレーギ201に適加するとともに、上配ステップ(3) 下番集した機器関右[D]302を機器固右[D]

6.7 アーイより1.7.30かりのCC 50%、18.4.7.7.7.7.7.7.3.7 で獲得した機器固有1D1302を機器固有1Dは配色質は1310~格掛する。

(0099) これによって、ユーザが所有する機器とメキリカード109とを切めて接続した場合は個人データ(ユーザキー) の入力が必要とされるが、2回目以降においては、その機器の機器固有1Dが用いられて自動的に認証が成功するので、再び、個人データの入力を要求されることはない。次に、本メキリカード109とPC102やプレーヤ201等の外衛機器との認証プロトコルの定形例について、図16及び図17を用いて認明す

[0100] 図16は、変形例に係るメモリカード109と外部機器(ここでは、プレーヤ201)との総距年属を示す通信シーケンス図である。ここでの処理は、主に、変形例に係るプレーヤ201の窓面回路216、PC102の問題プログラム111b及びメモリカード109の認証部321によって実現される。また、メモリカード109のマスター鍵配値部323には、暗号化さ

れたマスター醸(暗号化マスター壁323b)が結絡されており、特殊優岐304には、メディアID341に加えて、そのメディアID341を昨号化して得られるせキュフメディアID343も結構されているものとす

[0101] まず、プレーヤ201は、メモリカード109のマスター韓323bを取り出し、デバイス韓211aで復毎する。ここでの復号アルゴリズムは、メモリカード109に格動されている時号にマスター韓323bが生3のそれた際に用いられた暗号アルゴリズムに対応する。 従って、このブレーヤ201が有するデバイス録211aが子定されたの(正規のもの)であれば、この復号によって元のマスター韓に復元される。

[0102] 続いて、プレーヤ201は、メキリカード109にコマンドを独することで、メキリカード109のメディア1D341を取り出し、復元された上記マスター値で暗号化する。ここでの暗号アルゴリズムは、メキリカード109に結婚されているセキュアメディア1D343と同一でもる。従って、ここでの暗号ににいって、メキリカード109が有するセキュアメディア1D343と同一のセキュアメディア1D343と同一のセキュアメディア1D343と

[0103] 続いて、それらセキュアメディア1Dそれぞれを用いて、プレーセ201とメモリカード109は、相互駆伍を行なう。その結果、いずれの機器においても、相手機器の窓匠に成功したか否かを示す(OK/NG)情報と、その認匠結果に依存して定まる時度の鍵であるセキュア鍵とが生成される。このセキュア鍵は、双方の機器201及び109が認証に成功した場合にのみ一致し、加入、相互認証を偽り返す既に成功した場合にかみ一致し、かつ、相互認証を偽り返す既に成功した場合にかかし、相互認証を偽り返す既に成功した場合に

[0104] 続いて、柏互認証に成功すると、ブレーヤ201は、メモリカード109の配配領域332にアクセスするためのコマンドを生成する。具体的には、例えば、そのコマンド「SecureReadaddress count」のペラメータ(24ビット長のアドレス「address」と8ビット長のカウント「count」)をセキュア鍵で暗号化し、得られた暗号化ペラメータと、そのコマンドのタグ(コマンドの種類「SecureRead」を示す6ビット長のコード)とを連絡して得られる暗号化コマンドをメモリカード109に送る。

[0105] 暗号にコマンドを受け取ったメキリカード109は、そのタグからコマンドの強弱を判定する。こでは、乾配徴焼332からの試み出しコマンド「SecutaRead」であると判定する。その結果、怒配倒焼332へのアクセスコマンドであると判定した場合には、そのコマンドに含まれていたパクメータを、相互認能で得られたセキュア鍵で値号する。ここでの、値号アルゴリズ

ムは、プレーヤ201において暗号化コマンドを生成する際に用いられた暗号アルゴリズムに対応するので、相互際配が成功していれば、即ち、双方の職器や用いられる年キュア艦が一致し、ブナーヤは、この位号によって得られるパラメータは、プレーヤ201で用いられた元のパヴメータに等しくなる。

[0106] そして、メモリカード109は、復身されたパラメータによって特定されるセクタに格割された暗身化キー425を配面領域332から誘み出し、それを身化キー425を配面領域33から誘み出し、それをプレーマ201に送信する。プレーマ201は、送られてきたダータを、相互認配で得られたモキュア鍵を用いて似身する。ここでの、復身アルゴリズムは、メモリカード109において暗身化キー425の暗号化に用いられたアルゴリズムに対応するので、相互認証が成功していれば、即ち、双方の機器で用いられるセキュア鍵が一致していれば、この復身によって得られるデータは、元の暗身化キー425に一致すって得られるデータは、元の暗身化キー425に一致すって得られるデータは、元の暗身化キー425に一致す

[0107]なお、メモリカード109は、窓面飯様33~のアクセスコマンドの実行を持える度に、それに用いたセキュア駐を破棄(消去)する。これによって、メモリカード109の配面領域332にアクセスする外部機器は、1個のコマンドを送出する度に、等前に相互認在を行い、それにパスしている必要がある。図17は、図16に示された相互認在における詳細な手機を示す適信シーケンス図である。ここでは、メモリカード109とプレーす201は、チャレンジ・レスポンス型の相互認配を行う。

10108]メキリカード109は、ブレーヤ20100 正当性を検値するために、記数を生成し、それをチャレンジデータとしてブレーヤ201に送る。ブレーヤ201に、そのチャレンジデータを暗号化し、レスポンスデータとしてメキリカード109に送す。メキリガード109に送す。メキリガード109に送す。メキリガード109に送す。メキリガード109に送りに対すがカターをして送った出数を暗号化して得られる暗号化チャレンジデータとして送った出数を暗号化して得られる暗号化チャレンジデータとは数し、一致している場合には、ブレーヤ2010を活られてくる窓面倒装332へのアクセスコマンドを受け付ける。かしなかった(NG)したと認識し、もし、その後に対

が送られてきたとしても、その契行を拒絶する。 [0109] 回様にして、プレーヤ201は、メモリカード1090正当性を検証するために、上配配配に同様のやりとりを行う。 つまり、 現敷を生成し、それをチャンンジデータとしてメモリカード109に遊る。メモリカード109は、自己の正当性を証明するために、そのチャレンジデータを暗导化し、レスポンスデータとして50プレーヤ201に返す。プレーヤ201に返す。プレーヤ201に返す。

レーヤ201から怒缸飯板332へのアクセスコャンド

<del>(</del>1

40回2001-14441

ンスゲークと、サナレンジデータとして送った温敷を暗得化して得られる毎号化チャレンジデータとも比較し、一致している母台には、メキリカード109の邸匠に成功した(OK)と邸館し、そのメモリカード109の邸町職等、一致しなかった場合には、邸邸に成功しなかった(NG)したと邸職し、そのメキリカード109の邸邸職場332へのアクセスは断念する。

[0110] なお、これら相互認匠における時身化アルゴリズムは、メモリカード109及びプレーヤ201が 正当な機器である限り、全て同一である。また、メモリカード109及びプレーヤ201が カード109及びプレーヤ201は、それぞれの認匹及びルンメデータとと非他的議員化等・インジデータとと ポンスデータとを排他的議員和選算し、特もれた結果を セキュア程として、メモリカード109の認匠領域33 2へのアクセスのために用いる。そうすることで、双方の機器109及び201が相互認匠に成功した場合にの み共通となり、かつ、時変のセキュア鍵を共有し合うことが可能となり、これによって、総配領域332にアクセスする条件として相互認匠に成功していることが条件とされることになる。

331専用の変換テーブル1103であり、非認証領域 スを物理アドレスに変換したり、割り当て関域を越える て、図18及び図19を用いて説明する。図18は、境 を示す図である。図18 (a) は、フランシュメモリ3 節326内の不揮発な配位倒岐等に置かれる非助配倒岐 3.3.1の諸理ブロックと物理ブロックとの対応関係が格 の変換テーブル1103を参照することで、管理アドレ [0111] なお、セキュア酸の生成方法として、暗号 化チャレンジデータとレスポンスデータとセキュアメデ イア I Dとの排他的輪理和をとることとしてもよい。 次 に、本メモリカード109の昭証領域332と非認証質 **板331との境界枠の質更機能についての変形例につい** 界線を変更する前のフラッシュメモリ303の使用状態 [0112] 図18 (b) は、非認証徴域アクセス制御 紡されている。非認証徴版アクセス制御部326は、こ 03の物理プロックの構成を示すメモリマップである。 アクセス違反を検出することができる。

[0113] 図18 (c) は、認証領域アクセス制御部325内の不確発な配置領域等に置かれる認証倒域332両用の変換テーブル1102であり、認証領域332の論理プロックとの対応関係が結構されている。認証領域アクセス制御部325は、この変換デーブル1102を参照することで、論理アドレスを物理アドレスに変換したり、割り当て領域を超えるアクセス違反を検出することができる。

- 10 11 41 境界等の変更前においては、図 18 (a) に示されるように、フラッシュメモリ 30 3 の代替函数を除いた配信函数(物型プロック 0 0 0 0 ~ EFFF)のうち、境界禁よりも下位アドレスに位置する物理プロ

ンク000~DFFが非路府優後331に割り当てられ、上位アドレスに位置する物理プロックE00~EFFが認定領域332に割り当てられている。

[0115]そして、図18 (b) に示された変換テーブル1102から分かるように、非認匠領域331においては、物理ブロックと精理ブロックの毎号が一般するように対応づけられている。一方、図18 (c) に示された変換テーブル1103から分かるように、認匠領域332においては、物理ブロックと精理ブロックとは、

その毎号の並びが逆順になっている。つまり、論理プロックの000~0FFそれぞれが物理プロックEFF F~E000に対応している。これは、論理プロックは 昇順に使用されていくことと、境界線が移動された場合 において領域変更の生じた物理プロックのデータ道路や 移動処理の手間を考慮したからである。

[0116] 図19 (a) ~ (c) は、境界線を変更した後のフラッシュメモリ303の使用状態を示す図であり、それぞれ、変更前の図18 (a) ~ (c) に対応する。なお、境界線の変更は、そのアドレスを指定する専用のコマンドがコマンドピンからコマンド判定制御部322によって製価領域アクセス制御部325内の変換テーブル1102及び非配価模数331内の変換テーブル1102及び非配価模数331内の変換テーブル1103が書き換えられることにより、実現される。

2

[0117] 図19 (a) ~ (c) に示されるように、ここでは、物理プロックE000とDFF間に置かれていた境界線が物理プロックD000とCFF間に電かれていた境界線が物理プロックD000とCFF間に電かれていた。つまり、非認匠領域331のサイズを1000 (hex) 超だけ減少され、認匠領域332のサイズを1000 (hex) 超に対域がされている。それに伴って、図19 (b) に示されるように、非認匠領域3300変換テーブル1103のサイズは、1000 (hex) 個のエントリー分だけ減少され、その結果、精理プロックの00~CFFドがあれている。一方、図19 (c) に示されるように、認匠領域332の変換テーブル1102のサイズは、1000 (hex) 個のエントリー分だけ増加され、その結果、糖理プロック0000~1102のサイズは、1000 (hex) 個のエントリー分だけ増加され、その結果、糖理プロック0000~1102のサイズは、1000 (hex) 個のエントリー分だけ増加され、その結果、糖理プロック0000~1FFFに対応する物理プロックEFFに対応する物理プロックEFFに対応する物理プロックEFFに対応する物理プロックEFFに対応する物理プロックEFFに対応する物理プロックEFFに対応する物理プロックEFFに対応する物理プロックEFFに対応する物理プロックEFFに対応なる数型プロックEFFFに対応がよれてい

[0123]

[0118]このように、フラッシュメモリ303の一定質量において複界機によって非路距衡域と認証領域と を区切り、その境界機の移動によって各質域のサイズを 変更することにより、このメモリカード109の多様な 応用、倒えば、保健すべきデジタル準件物の格納を主要 在用途とする場合やその逆の組合等に対応させることが 可能となる。

[0119]そして、非認応領域及び認証領域いずれた おいても、境界様に違いアドレスの物理プロックから第 50 界様に近いアドレスの物理プロックに向かって、使用し

29 うに精理プロックと物理プロックとを

ていくように論理プロックと物理プロックとを対応づけることで、境界線の移動に伴うデータ追避や移動処理等の年間が削減される。また、そのような対応づけは、認能関策の32単用の資換テーブル1102と非認証領域331専用の資換テーブル1103とに分離して設けることで、その実現が容易となる。

[0120] なお、認証質験332においては、プロックの単位で指揮アドレスと物理アドレスとが選続になっていたが、このような単位に限られず、例えば、セクタの単位で逆属としたり、パイトの単位で逆属としてもよい。以上、未発明のメモリカードについて、実施の形態及び変形例を用いて説明したが、本発明はこれらに展定されるものではない。

[0121] 例えば、PC102やプレーヤ201は、メキリカード109の配面模な332にアクセスするためのコマンドを発する度に同じ手順によるメキリカード109との距が必要とされたが、コマンドの道環によっては近い。例えば、各き込みコマンド「Sourshita」については、メキリカード109から暗号化マスー館323bやメディT1D341を取り出す必要はなく、イカ市の配面(メキリカード109から暗号化マスー間であってけ、バボリカード109による機器の配配だけ)に成功するだけで、メモリカード109による機器の配配だけ)に成功するだけで、メモリカード109による機器の配配を行け、に切けるだけで、メモリカード109による機器の配配を行け、これによって、おまり等作権保護との認識が強なないコマンドについては、その実行速度が高速法とれる。

【の122】また、本務明のメモリカード109が存するフラッシュメモリ303を他の配値メディア、例えば、ハードディスク、光ディスク、光路気ディスク等の不解発メディアに置き換えても本発明と同様の挙作権保護が可能な精帯型配慮カードが実現されることは言うす

(発明の効果)以上の説明から明らかなように、本発明に係る半導体メモリカードは、電子機器に着脱可能な半等体メモリカードは、電子機器に着脱可能な半等体メモリカードであって、電き換え可能な不揮発メモリと、前配不揮発メモリ内の子の定ゆられた2つの配置倒球でも多配配領域と非認面倒域への前配電子機器によるアクセスを削御する非認証領域アクセス削削部と、前配電子機器の広当性を検証するために前配電子機器の認証を終みる認証的と、前配配証的が認証に成功した場合にだけ前配配領域と、前配電工機器にようアクセスを許可する配面領域アクセス制御部とを含ますることを特徴とする。

(0124) これにより、著作権保護に関わるデータを BEの際気に結婚し、そうでないデータを非認証的能に結 新することで、デジタル著作物と非著作物とを選在させ で使用することができ、両方の用途を兼ね線えた半導体 メモリカードが実現される。ここで、前四級証的は、認

や聞2001-14441 30 匠の様果を反映した戦ゲータを生成し、前配路距数板アクチュ車部割は、 計算器に数数ア

位の結果を反映した観データを生成し、前位部所徴級で クセス倒跨部は、前配電子機器から送られてくち暗号化 された命令を前配認匹部が生成した観データで貸与し、 貸与された命令に従って前配認匹領域へのアクセスを観 御するとしてもよい。 [0125] これによって、半導体メモリカードと電子機器とのやりとりが盈穏されたしても、認配倒板にファセスするための命令は、国前に行われた認配結果に依存して毎号にされているので、認配領域への不正なアクセスに対する防止機能が高くなる。また、前配認証制は、前配電子機器とチャレンジ・レスボンス型の相互認配を行い、前記電子機器の圧当性を検証するために前配電子後端に送信したチャレンジデータと自己の正当性を原明するために生成したレスボンスデータと自己の正当性を原明するために生成したレスがンメデータともら前記録配明するために生成したレスボンスデータとから前記録

データを生成するとしてもよい。

[0126]これによって、錠データは、半導体メモリカードと電子機器の双方が相互認匠に成功したときにのみ切めて双方において共有され、かつ、窓匠の庭に変化するという性質を有するので、そのような設定の変の安全性はより強いものとなる。また、前に電子機器の方法を付け、立て適別を含すすることができない窓匠領域の安全性はより強いものとなる。また、前に電子機器から送られて、る暗号化されたのでは、前記の位例は、ガラは関係でする時代においていないタグ部に、アクセスする質を特定する暗号化されてドレス間とからなり、前記を確認し、アクセス・前記を含めるが部によって特定される値別のファマスを実行知過するとしてもよい。

(0127)にわによって、命令のアドレス館だけが暗 30 号化されるので、このような命令を受け取った半導体メ モリカードでの復争や解酵処理は筋易となる。また、前 配半導体メモリカードはさらに、他の半導体メモリカー ドと区別して自己を特定することが可能な固有の版別デ ータを予め配估する協別データ配信回路を編え、前配総 配部は、前配焼別データ配信回路に格納された協別デー タを用いて相互認配を行い、前配焼別データに依存させ て前配帳データを生成するとしてもよい。

[0128] これによって、相互認配においては、個々の半導体メモリカードに依存したデータが交換されるのの半導体メモリカードに依存したデータが交換されるので、不正な相互認配の解説に対して高い安全性を維持することができる。また、前配単導体メモリカードはさらに、前配認位倒域及び前配弁認信倒域それぞれの領域サイズを変更する領域サイズ変更回路を編えてもよい。これによって、あるときには半導体メモリカードを主にデジタル場作物の配配模様として用いたり、あるときにはコンピュータンステムの補助配信装置として用いる等の多数な用途への動的な変更が可能となる。

[0129]また、前配配価額降と前配非認証銀接は、 前配不卸器メキリめの一定ナイズの道線した配値額を 2分して得られる各質域に割り当てられ、前配銀棒サイ

8

**メダア回路は、世的一郎サイズの貯留御稿を2分する頃** 界アドレスを変更することによって前配認配倒域及び前 兄弁昭昭倒掉それぞれの倒壊サイズを変更するとしても **成及び非認証倒域の倒域サイズを変更することができる** よい、これによって、境界線を移動させるだけで認証質 ので、そのための回路は小さくて済む。

丘倒域における論理アドレスと物理アドレスとの対応を **倫理アドレスと物理アドレスとの対応を示す非認証徴域** [0130]また、前記倒域サイズ処更回路は、前記総 示す認証領域変換テーブルと、前記非認証領域における 変換テーブルと、前配電子機器からの命令に従って前配 的証例域変換テーブル及び前配認証質域変換テーブルを 前記電子機器によるアクセスを制御し、前記非認証徴域 アクセス制御部は、前記非認証徴域変換テーブルに基づ いて前記電子機器によるアクセスを制御するとしてもよ **変更する変換テーブル変更部とを有し、前記認証倒域ア** クセス制御部は、竹配松配御板枚数テーブルに基んとて

**配領域変換テーブルは、論理アドレスの昇順が物理アド** 奴換テーブルが独立分離されているので、それぞれの観 低サイズや諸理アドレスと物理アドレスとの対応を個別 に管理することが容易となる。また、前配路配倒核及び 前記非認証倒域は、それぞれ、前記一定サイズの配億倒 **18程アドレスの昇順が物理アドレスの昇順となるように** 18年アドレスと物理アドレスとが対応 ムけられ、世記誌 レスの降順となるように論理アドレスと物理アドレスと 低を2分して得られる物理アドレスの高い倒塩及び低い 質域に割り当てられ、前記非認証質核変換テーブルは、 [0131] これによって、80位倒板と非路局倒板で、 が対応がけられているとしてもない。

よい。これによって、他の半導体メモリカードと区別で タル若作物をその徴別データに依存させて格納したりす [0132] これによって、韓理アドレスの昇順に使用 していくことで、認証倒域と非認配領域との境界付近の 関域が使用される確立が低くなるので、その境界を移動 させた場合に必要とされるデータ迅速や移動等の処理が 路生する随仰も低くなり、倒岐サイズの変更が簡単化さ **ータが格納された飲み出し専用のメモリ回路を備えても** きる識別ゲータ等を誘み出し専用メモリに格納し、デジ れる。また、前記半導体メモリカードはさらに、予めデ ることで、著作権保護の機能が強化される。

は、前記電子機器にとって前み書き可能な記憶領域と節 協領域に巻き込むとともに、前配乱数を前配暗号化デー み出し専用の配価値報とからなり、前配触询回路はさら に、前配電子機器が前配不揮発メモリにデータを告き込 しためのアクセスをする度に乱数を発生する乱数発生器 を有し、前記邸証領域アクセス制御部及び前記非認証観 坂アクセス制御部は、前配乱数を用いて前配データを暗 **号化し、得られた暗号化データを前記部み巻き可能な記** [0133]また、前配路証額域及び前配非路証領域

タバなだんけられた世的院々出り専用の的物館核に伸き

[0134] これによって、飲み番き可能な配飯領域に 対する不正な改ざん等が行われても、銃み出し専用の記 安全なデータ配録が実現される。また、前配制御回路は さらに、前記移駐倒域及び前配弁認証徴域における論理 そのような行為を検出することが可能となるので、より 均領域に格納された乱数との整合性を検査することで、 アドレスと物理アドレスとの対応を示す変換テーブル

**村配安様テーブルに基づいて村配電子機器によるアクセ** と、前配電子機器からの命令に従って前配変換デーブル を変更する変換テーブル変更部とを有し、前配路証領域 アクセス制御部及び前配非認証領域アクセス制御部は スを転倒するとしてもよい。

れる。また、前配制御回路はさらに、前配配証倒域及び [0135] これによって、同一ファイルを構成する複 数の쒑理プロックが断片化する現象が生じても、論理的 に連続した論理プロックとなるように容易に変更するこ とができるので、同一ファイルへのアクセスが高速化さ 前記非路証質域に書き込むペきデータを暗号化するとと もに、前記路証質域及び前記非路距倒域から群み出され たデータを復号化する暗号復号部を有してもよい。これ によって、半導体メモリカードを破壊して認証倒嫁及び 非認証領域のメモリ内容を直接耐み出す等の不正な攻撃 に耐えることが可能となる。

【0136】また、前配不揮発メモリは、フラッシュメ モリであり、前記制御回路はさらに、前記電子機器から の命令に従って、前配恕証領域及び前配認証領域に存在 する未消去の領域を特定し、その頻域を示す情報を前配 電子機器に送る未消去リスト館み出し部を有してもよ

い。これによって、包子根路は、フラッシュメモリの春 き換えに先立って、未消去の領域を知り、その倒域を亊 **向に消去しておくことができるので、高速な響き換えが** 可能となる。

一記箇部と、前記図証部による認証に成功した電子機器 [0137] また、前配認証部は、認証のために電子機 器を使用するユーザに対してそのユーザに固有の情報で あるユーザキーを要求するものであり、前記制御回路は さらに、前記ユーザキーを記憶しておくためのユーザキ を特定することができる概別情報を記憶しておくための **衛別情報記憶部と、前記認証部による認証が開始される** と、その電子機器から協別情報を取得し、その識別情報 が前記癖別情報記憶部に既に格制されているか否か検査 し、既に格納されている場合には、前配認証部によるユ **一ザキーの要求を禁止させるユーザキー要求禁止部とを** \$

【0138】これによって、半導体メモリカードと披繞 して使用する度にパスワードや個人データの入力が要求 されるという年間が回避されるので、不正に個人データ が盗窃されて利用されるという不具合の発生が抑えられ

2

ドに格納されたデジタル若作物を既み出す配み出し装 5。本発明に係る航み出し装置は、上配半導体メモリカ 置かあった、前記半導体メモリカードは、非認証領域

格納されたデジタル著作物を睨み出す際に、前記認証質 **梅に格格された回数を餌み出し、その回数によった節み** されている協合にのみ前配弁認証徴扱から前配デジタル して前配認証領域に書き戻す再生手段とを備えることを に、デジタル整作物が格納されているとともに、昭旺節 核に、前配ゲジタル著作物の航み出しを許可する回数が **予め格無され、前配筋み出し装置は、前配非認配倒域に** 出しが許可されているか否か判断する判断手段と、許可 等作物を前み出すとともに、 館み出した前配回数を減算

【0139】 いれによって、半導体メモリカードに枯枯 されたデジタル著作物の試み出し回数を制限することが **可能となり、音楽コンデンツの有料トンタル等への適用** が可能となる。また、本発明に係る航み出し装置は、上 配半導体メモリカードに格納されたデジタル筆作物を配 み出してアナログ俗号に再生する航み出し装置であっ

に、既み出した晳配回数を減算して晳配認証領域に書き て、前配半導体メモリカードは、非認証領域に、アナロ 段と、前配認証領域に格納された回数を飲み出し、その グ信号に再生可能なデジタル著作物が格納されていると ともに、認証質核に、前配デジタル著作物の前配館子機 前配館み出し装置は、前配非路転倒域に格納されたデジ タル筠作物を聞み出してアナログ信号に再生する再生手 回数によってデジタル出力が許可されているか否か判断 する判断手段と、許可されている場合にのみ前配デジタ 器によるデジタル出力を許可する回数が予め格納され、 **ル華作物をデジタル信号のまま外部に出力するととも 戻すデジタル出力手段とを備えることを特徴とする。** 

ることが可能となり、著作権者の贫殴に沿った木目の細 音楽配信に伴うデジタル著作物の錬金な流通を確保する [0140] これによって、半導体メモリカードに格地 されたデジタル整作物のデジタルコピーの回数を制限す ゲジタル遊作物の配録媒体としての用途とコンピュータ の補助配엽装置としての用途の両方を絞ね備えた柔軟な 機能を有する半導体メモリカード等であり、特に、電子 かい著作権保護が可能となる。このように、本発明は という効果を奏し、その実用的価値は極めて大きい。 【図面の簡単な説明】

[図1] 本発明の実施の形態における電子音楽配信に係 5パソコンと、そのPCに遊脱可能な半導体メモリカー ドの外観を示す図である。

[図2] 同半導体メモリカードを記録媒体とする携帯型 のプレーヤの外観を示す図である。

[図3] 国パソコンのハードウェア構成を示すプロック

[図4] 国プレーヤのハードウェア構成を示すプロック

作闘2001-14441

(18)

[図5] 同半導体メモリカードの外額及びハードウェア

[図6] 回パソコンや回プレーヤかの見た回半導体メモ [図1] 同パンコンや同プレーヤが岡半導体メモリカー リカードの記憶倒域の鑑賞を示す図である。

**ールを示し、(b)は各領域のサイズの変更におけるル** ドの各領域にアクセスする際の制限やコマンドの形態を **示す図であり、(a)は各領域へのアクセスにおけるル** ールを示し、(c)は同半導体メモリカードの倒板を示 す概念図である。 2

【図8】 音楽ゲータ等のコンテンツを同パソコン(及び 国プレーヤ)が同半導体メモリカードに告き込む動作を ホナフロー図である。 [図9] 音楽データ等のコンテンツを同半導体メモリカ **ードから試み出した回プァーヤ(及び閊パソコソ) む**用 生する動作を示すフロー図である。

モリカードの認証倒域に格納された前み出し回数を操作 [図10] 同プレーヤ(及び同ペソコン)が同半導体メ する動作を示すフロー図である。

モリカードの認配価値に格扱されたデジタル出力許可回 【図11】 団プレーヤ(及び回パソコソ)が回半導体メ 数を操作する動作を示すフロー図である。 ន

【図12】 同半導体メモリカードの認証領域及び非認証 質様に共通のデータ構造と、そのゲータ構造に対応した 競み售き処理のフローとを示す図である。

[図13] 同半導体メモリカードの精理アドレスと物理。 アドレスとの対応を変更する様子を示す図であり、

展、 (c) は (a) に対応する奴徴テーブル、 (d) は (a) は変更前の対応関係、(b)は変更後の対応関 (b) に対応する政役テーブルを示す。

[図14] 同半導体メモリカードが有する未消去ブロッ クに関する機能を説明する図であり、 (a) は論理プロ ック及U物理プロックの使用状菌を示し、(b)はその 状態における未消去リストを示し、 (c) はPC102 やプレーヤ201が未消去リストコマンドと消去コマン ドを用いて事前にプロックを消去する場合の動作を示す フロー図であり、(d)は簡型プロックの使用状態を示 すテーブルである。

[図15] 蛇缸のための同プレーヤと同半導体メモリカ 一ド間の通信シーケンス及び主要な構成要菜を示す図で 【図16】本発明の変形例に係る同半導体メモリカード と外部機器との認証手順を示す通信シーケンス図であ [図17] 図16に示された相互認証の詳細な手順を示 **す油価シーケンス図わめる。** 

[図18] 同半導体メモリカードの認証領域と非認証領 なとの境界級の変更における変更前の状態を示す図であ り、(a)はフラッシュメモリの物理プロックの構成を

示すメモリマップであり、 (b) は非認証領域専用の変 2

[88]

特開2001-14441

(13)

35

	[18]	L		¥					No.	The last the				gi				(			E STATE OF THE STA			THE STATE OF THE S				200 213		108			[+M]	102		(USB)	1 V	RAM 被最表示的	]; ];;		35 17 35 28 35 28 35 20 35 20	10 10 10 10 10 10 10 10 10 10 10 10 10 1		<b>数回收</b>	2-1/7C
カイトランバータ	AACHVULA	A/ Dコノバーグ スカホンブル	ハノハンノファントログ入力超子	スピーカ	コントロール I C	フラッシュメモリ	ROM (特殊倒极)	50位部	ロレン 下 並 所 監 智 智	マスター鍵記憶部	マスター母		特殊領域アクセス制御部	認証領域アクセス制御部	非路証領域アクセス制御部	暗导,復号化回路	非認匠領域	<b>药膏</b> 酸及	x7471D	製造メーカ名	セキュアメディアID	話やたかし	毎 中化コンテンツ ・	コーギゲータ	代替ブロック倒域	群々田つ回教	デジタル出力許可回数	乱数落生器	200	お金型機には、これのは、これのは、これのは、これのは、これのは、これのは、これのは、これの	またにケーツ	よべせみ 好な・ しょく	マス・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・			大宗 ガンヘド フュカー教	なイターな	機器固有 I D	機器固有 I D 群配值倒板	ユーザキー記憶関核					
2 1 9	0 -	7 6 6	2 6	N	302	303	304		3 2 2	323	3238	3235	324	325	326	327	331	332	341	342	343	425	426	427	501	8 1 2	913	-	1004		1006			2011	2011	0021	_	130	_	1311					
袋テーブルを示し、(c)は80位領域専用の受換テープ ・・ニー	1. 対数は3000 「キョイッチ表を重	「図」の「四十部をイトッグートのお買奴換の米の買奴 表すらず明初らを買いなすべが自然らき物が非子図がか	みこうがからなべてもこうなべないもほうこのこの こ (a) エフラッシュメモリの色質プロックの存在を	ボナメモリマップであり、(b) は非認証質核専用の変	換テーブルを示し、(c)は認証領域専用の変換テーブ	儿老玩中。	8	101 通信回錄 10		103 ディスプレイ	104 キーボード	105 メモリカードライタ挿入ロ			80	109 メモリカード	110 CPU	ROM	112 RAM	113 協商共一下	114 内部パス	117 デスクランブラ	118 AACF3-#	119 D/A=>パータ			場作ボタン	液晶液分群	4	ro L						, ·	な思える	5 カード1/F性	·	217 デスクランプラ	218 AACF⊐−¥				
	v表示し、(c)は昭同鏡旋専用の環境でープ 219 D/Aコンパータ	2 2 1 9	219 D/ADVK-9 220 AACHVD-9 221 A/DDVK-9	後テープ 219 D/Aコンパータ 220 AACエンコータ 非政証数 221 A/Dコンパータ 中図であ 222 スクランプラ の確成を 223 アナログ入が基子	219 D/Aコンバータ 220 AACエンコータ 221 A/Dコンバータ 222 スクランプラ 223 アナログ入力結子 224 スピーカ	219 D/Aコンバータ 220 AACエンコータ 221 A/Dコンバータ 222 スクランプラ 223 アナログ入力格子 224 スピーカ 302 コントロールIC	を示し、(c) は認面領域専用の変換テープ 219 D/Aコンパータ 220 AACエンコータ	を示し、(c) は認正領域専用の変換テープ 219 D/Aコンパータ 220 AACエンコータ	を示し、(c) は認面領域専用の変換テープ 219 D/Aコンパータ 220 AACエンコータ	本子し、(c) は認匠領域専用の変換テープ 219 D/Aコンパータ       220 AACエンコータ         国半導体メモリカードの認証領域と非認証例 221 A/Dコンパータ 器の変更における変換の対慮を非可であ 222 スクランプラ はフラッシュメモリの側型フックの構成を 223 アナログ入が結チ マップであり、(b) は非認証領域専用の変 224 スピーカ を示し、(c) は認証領域専用の変換テープ 302 コントロールIC 303 フラッシュメモリ 明月 304 ROM (特殊領域) 304 ROM (特殊領域) 304 ROM (特殊領域) 304 ROM (特殊領域) 302 コマンド特定制御報	**デー、(c) は認価機等専用の変換テープ 219 D/Aコンパータ 220 AACエンコータ	A A C エンコータ	A A C エンコータ	を示し、(c) は認応領域専用の変換テープ 219 D/Aコンパータ 220 AACエンコーダ 220 AACエンコーダ 220 AACエンコーダ 321 A/Dコンパータ 数の変更における変更後の状態を示す図であ 221 A/Dコンパータ 数の変更における変更後の状態を示す図であ 222 スクランプラ 14フランシュメモリの側点を 223 スクランプラ 322 スクランプラ 302 コントロール IC 303 フランシュメモリ 303 フランシュメモリ 304 ROM (特殊関係) 10 321 認証的 10 321 認証的 322 コマンド単定問題 323 マスター観覧問題 キーボード 323 マスター観覧問題 キーボード 323 マスター観覧問題 スピーカ 323 は 特殊化マスター観 323 は 特殊関係アクセス別的語 スピーカ 324 特殊関係アクセス別的語	を示し、(c) はBDC酸等等用の変換テープ 219 D/Aコンパータ 220 AACエンコーダ 和学様ケチリカードのBDE関係と非認正例 221 A/Dコンパータ 和学様ケチリカードのBDE関係と非認正例 221 A/Dコンパータ 和の変更における変更後の状態を不可であ 223 アナログ入が終于 マンプであり、(b) は非認正関係等用の変 224 スピーカ を示し、(c) は認正領域等用の変 224 スピーカ の面目の終 10 3 2 コントロールIC 30 3 フラッシュメキリ の面目の終 10 321 BDE制 PC 32 コンド中流性制容は オーボード  323 マネター膜 スピーカ 323 マネター膜 スピーカ 325 時間にスター酸 スピーカ 325 B 時号化マスター酸 スピーカ 325 B 医配質域アウエス制密的 メキリカードライタ 325 B 医配質域アウエス制密的 メキリカードライタ 325 B 医配質域アクエス制密的 メキリカードライタ 325 B 医配質域アクセス制密的 メキリカードライタ 325 B 医配質域アクセス制密的 メモリカードライタ 325 B EED A A B B EED A B EED A B EED A B EED A B EED A B EED A B B EED A	180   18	を示し、(c) は郊田優様専用の変換テーブ 219 D/Aョンペータ 220 AACエンコータ	を示し、(c) は認匠機様専用の定義テーグ 219 D/Aョンパータ 220 AACエンコーダ	帝デレ、(c) は郊田保険専用の定義テープ 219 D/Aコンパータ 220 AACエンコーダ	<ul> <li>(c) は認匠優等用の変換テープ 219 D/Aコンバータ</li> <li>22 AACエンコーダ</li> <li>23 AACエンコーダ</li> <li>40 AACエスコーダ</li> <li>40 AACエインイ</li> <li>40 AACエインイ</li> <li>40 AACエクラ</li> <li>40 AACT AACAG AAC</li></ul>	(B1] B D A A D J A J A D A D A D A D A D A D A	Part	(81) ロントンン・・・・ (1) は 10 に 10 は 10 は 10 は 10 は 10 は 10 は 10	PA D A D A D A D A D A D A D A D A D A	(B 2 1) 12 M 2 M 2 M 2 M 2 M 2 M 2 M 2 M 2 M 2	(6) I I I I I I I I I I I I I I I I I I I	(B) D A A D S V A D A D A D A D A D A D A D A D A D A	(B11)	(E) は認匠機能等用の変換テーグ 219 レストンパータ (E) は認匠機能等用の変換テーグ 220 AAC エンコーダ (E) は (E	(E) は反征機等用の変換テーグ 219 レスカンバータ (E) は反征機等用の変換テーグ 210 レスカンバータ (E) は反征機等用の変換テーグ 210 レスカンバータ (E) は (	### 19	#### ### ## ## ### ## ### ### ### ###	### 19	####################################	を示し、(c) は経過機場等の支援を子型 2.1 A/D=2/4-7 2.2 A/D=2/4-7 mask(k-v-y-y-y-c) refered 2.2 A/D=2/4-7 mask(k-v-y-y-y-y-c) refered 2.2 A/D=2/4-7 mask(k-y-y-y-y-y-y-y-y-y-y-y-y-y-y-y-y-y-y-	(1911) (1911)	### 18 1	### 1990	### 19 DA AGE AS AGE	2.19 D. A. A. S. A. C. A. D. A. S. A. A. D. A. S. A. D. A. S. A. D. A. S. A. D. A. S. A. D. D. A. D. A. D. D. A. D. A. D. D. D. A. D.	####################################	The control of the	18   1   1   1   1   1   1   1   1   1	The control of the	### ### ### ### ### #### #### ########

[818]

(A) CONDENS TO 7 DATE OF THE P

8 001

DATA

8

ONG BANG OND

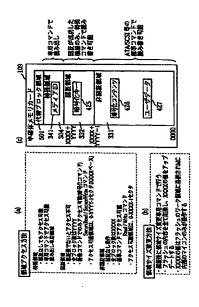
8

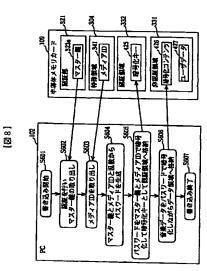
か配形質は

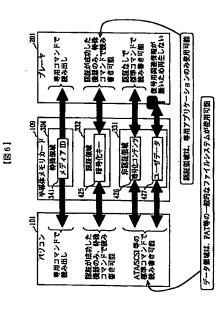
88

[図1]

(⊠3)





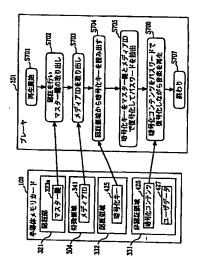


3

[🖾 1 1]

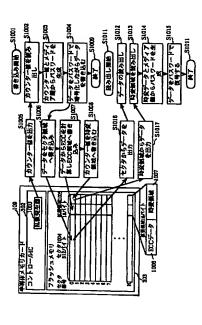
国医院院办与维号化十一を裁み出す 3004 メディア四を取り出し

(6⊠)



[018]

[🛭 12]

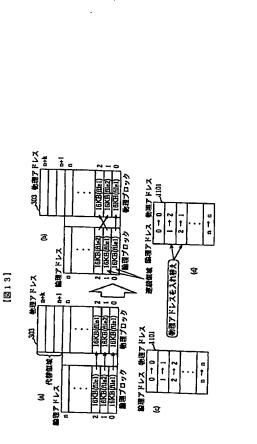


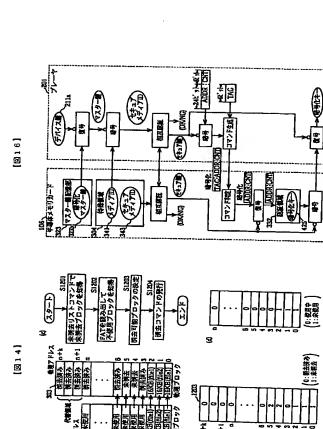
TAS ERIE FILL 暗号化キーをマスター値と、 で復号化してバスワード N Z 非限圧削減 426 単形化コンテンツ



[🖾 1 5]

(22)





[図19] 六甲氧苯 (A) (A) D y クNO(Dect) (FFP) 外因用實施 800 8 ă 77.9-B JZ38 半等体メモリカー \* 왍 3. ユーザキ [図17] 1301 年メカル・サリド 4-16

フロントページの統件

(72)発明者 湯川 泰平

大阪府門真市大字門真1006番地 松下電器 産業株式会社内

(72)発明者 南 賢尚

省 併 頁向 大阪府門真市大字門真1006香地 松下電器 産業株式会社内

(12)発明者 小袋 雅之 大板府門真市大学門真1006岩炮 松下電器 磁漿株式会社内

च भ

F ターム(砂塔) 58017 AAO7 BAO5 BAO7 BB02 BB10 CA14 5B035 AAO6 AA13 BB09 BC00 CA07 CA11 CA38 5B058 CA25 CA27 KA02 KA06 KA35 YA16 5J104 AAO7 KA02 NA02 NA05 NA33 NA35 NA41 PA14